Department of Homeland Security

Information Analysis and Infrastructure Protection Directorate

CyberNotes

Issue #2003-09 *May 5, 2003*

CyberNotes is published every two weeks by the Department of Homeland Security/Information Analysis and Infrastructure Protection (IAIP) Directorate. Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between April 9 and May 1, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
360 Degree Web[1]	Windows XP	Platinum Key	A vulnerability exists in the smart card security application due to insufficient access restrictions, which could let a malicious user obtain sensitive information and obtain access to the task bar and potentially execute applications.	No workaround or patch available at time of publishing.	PlatinumKey Access Control Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[1] Bugtraq, April 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
3D-FTP[2]	Windows	3D-FTP Client 4.0	A buffer overflow vulnerability exists due insufficient bounds checking on banner data, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	3D-FTP Client Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Adobe Systems, Inc.[3] ***Upgrade available & exploit virus***[4]	**Windows 95/98/NT 4.0/2000, XP, MacOS, Unix**	**Acrobat 4.0 5, 4.0 5c, 4.0, 4.0.5 a, 5.0, 5.0.5, Acrobat Reader 4.0 5, 4.0 5c, 4.0, 4.0.5 a, 5.0, 5.0.5**	**A vulnerability exists in the implementation of the certification mechanism due to a failure to check the validity of a plug-in, which could let a malicious user produce false digital signatures to enable execution of arbitrary code.**	**Update available at:** http://www.adobe.com/support/downloads/detail.jsp?ftpID=2121	**Acrobat Plug-in Digital Signature** **CVE Name: CAN-2002-0030**	**High**	**Bug discussed in newsgroups and websites.** ***The W32/Yourde Virus exploits this vulnerability.***
Alt-N Technologies[5]	Windows	MDaemon 6.0.7, 6.5.0, 6.7.5, 6.7.9	A buffer overflow vulnerability exists in the 'DELE' and 'UIDL' server commands due to inadequate bounds checking, which could let a remote malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	MDaemon 'DELE' & 'UIDL' Commands Buffer Overflow	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Alt-N Technologies[6]	Windows	MDaemon 6.7.5, 6.7.9	A buffer overflow vulnerability exists due to a boundary error in the IMAP service, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	MDaemon IMAP Server Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Alt-N Technologies[7]	Windows	WebAdmin 2.0 0-2.0.2	A vulnerability exists because an HTTP request can be submitted that will return the contents of any web server readable file, which could let a remote malicious user obtain sensitive information. *Note: The user must have administrative privileges in WebAdmin in order to access these files.*	Upgrade available at: http://www.altn.com/download/default.asp#WebAdmin	WebAdmin Remote File Disclosure & Viewing	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
AN-HTTPd[8]	Windows 95/98/ME/ NT 4.0/2000, XP	AN AN-HTTPd 1.2b, 1.2.1, 1.38-1.40, 1.41b -1.41e, 1.41, 1.42f-1.42h	A Directory Traversal vulnerability exists in the 'count.pl' sample script due to insufficient access validation, which could let a remote malicious user create or overwrite user-specified files.	No workaround or patch available at time of publishing.	AN HTTPD 'Count.pl' Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[2] Bugtraq, April 28, 2003.
[3] ElcomSoft Co. Ltd. Security Notice, March 24, 2003.
[4] SecurityFocus, April 30, 2003.
[5] Damage Hacking Group Security Advisory, April 26, 2003.
[6] Damage Hacking Group Security Advisory, April 27, 2003.
[7] Bugtraq, April 25, 2003.
[8] Bugtraq, April 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Foundation[9, 10]	Unix	Apache 2.0.39-2.0.44	A vulnerability exists because file descriptors are inherited by child processes, which could let a malicious user obtain sensitive information.	**Apache:** http://www.apache.org/dist/httpd/ **RedHat:** ftp://updates.redhat.com/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/	Apache Web Server File Descriptor Leakage	Medium	Bug discussed in newsgroups and websites.
Apple[11] ***Exploit script has been published[12]***	**MacOS X 10.x**	**MacOS X 10.0-10.2.4, MacOS X Server 10.0, 10.2-10.2.4**	**A remote Denial of Service vulnerability exists in the Directory Service daemon when a malicious user repeatedly connects to specific network ports.**	**Upgrade available at:** **http://docs.info.apple.com/article.html?artnum=120211**	**MacOS X Directory Service Denial of Service**	**Low**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***
AStArt Technologies[13] ***RedHat issues advisory[14]***	**Unix**	**LPRng 3.8.10 .1**	**A vulnerability exists in the 'psbanner' filter because temporary files for debugging purposes are created insecurely, which could let a malicious user obtain elevated privileges.**	**Debian:** **http://security.debian.org/pool/updates/main/l/lprng/** ***RedHat:*** **ftp://updates.redhat.com**	**LPRng 'PSBanner' Insecure Temporary File Creation** **CVE Name: CAN-2003-0136**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Auerswald[15]	Windows	COMsuite 3.1 06/2001	A vulnerability exists because a weak default password is created to enable operating system interaction, which could let a local/remote malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	COMsuite Weak Default Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Battleaxe Software[16]	Windows	bttlxe Forum	A vulnerability exists in the 'login.asp' page due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	BTTLXE Forum Login.ASP CVE Name: CAN-2003-0215	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
BRS[17]	Windows	Web Weaver 1.04 & prior	A remote Denial of Service vulnerability exists when a malicious user tries to retrieve a non-existing file.	No workaround or patch available at time of publishing.	WebWeaver Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[9] Red Hat Security Advisory, RHSA-2003:139-01, April 9, 2003.
[10] Conectiva Linux Security Announcement, CLA-2003:632, April 30, 2003.
[11] @stake, Inc. Security Advisory, a041003-1, April 10, 2003.
[12] SecurityFocus, April 23, 2003.
[13] Debian Security Advisory, DSA 285-1, April 14, 2003.
[14] Red Hat Security Advisory, RHSA-2003:142-01, April 24, 2003.
[15] SySS-Advisory, April 29, 2003.
[16] SecurityTracker Alert ID, 1006632, April 23, 2003.
[17] Bugtraq, April 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Central Command[18]	Unix	Vexira Antivirus for Linux 2.1.7	A buffer overflow vulnerability exists when an overly long commandline argument is submitted to the Vexira binary, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Vexira Antivirus Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Cisco Systems[19]	Multiple	Catalyst 4000 7.5 (1), 6000 7.5 (1), 6500 7.5 (1)	A vulnerability exists due to the way the 'enable' mode is accessed, which could let a remote malicious user obtain elevated privileges.	Workaround available at: http://www.cisco.com/warp/public/707/cisco-sa-20030424-catos.shtml.	CatOS Authentication Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Cisco Systems[20]	Windows NT 4.0/2000	Secure ACS for Windows NT 2.1, 2.3-2.6, 2.6.2-2.6.4, 3.0.1, 3.0, 3.0.3, 3.1.1	A buffer overflow vulnerability exists due to a boundary error in the 'CSAdmin.exe' administration service listening on port 2002/tcp, which could let an unauthorized remote malicious user cause a Denial of Service and potentially obtain administrator access.	Patches available at: http://www.cisco.com/cgi-bin/tablebuild.pl/cs-acs-win	Cisco Secure ACS Management Interface Buffer Overflow CVE Name: CAN-2003-0210	Low/**High** **(High if adminis-trative access can be obtained)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Compaq[21]	Unix	Compaq Tru64 4.0 g PK3 (BL17), 4.0f PK7 (BL18), 5.0a PK3 (BL17), 5.1b PK1 (BL1), 5.1a PK4 (BL21), 5.1 PK6 (BL20)	A vulnerability exists in the 'dupatch' and 'setld' utilities that are used during update and installation procedures, which could let a malicious user cause a Denial of Service or obtain elevated privileges.	For workaround, see advisory located at: http://thenew.hp.com/country/us/eng/support.html Input "SSRT3471" in the "Search" box	Tru64 Installation Software Insecure File Creation	Low/ Medium (Medium if elevated privileges can be obtained)	Bug discussed in newsgroups and websites.
Debian[22]	Unix	mime-support 3.9-3.21	A vulnerability exists in the 'mime.types' and mailcap' control files due to invalid sanity checks when creating temporary files, which could let a malicious overwrite arbitrary files.	Upgrade available at: http://http.us.debian.org/debian/pool/main/m/mime-support/	MIME-Support Insecure Temporary File Creation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Deerfield.com[23]	Windows 95/98/ME/ NT 4.0/2000, XP	VisNetic Active Defense 1.3.1	A remote Denial of Service vulnerability exists due to an error in the handling of long HTTP GET requests.	Patch available at: ftp://ftp.deerfield.com/pub/current/vad_131_patch.exe	VisNetic ActiveDefense HTTP Get Requests Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[18] Securiteam, April 18, 2003.
[19] Cisco Security Advisory, Revision 1, April 25, 2003.
[20] NSFOCUS Security Advisory, sA2003-04, April 24, 2003.
[21] HP Security Bulletin, SSRT3471, April 28, 2003.
[22] Debian Security Advisory, DSA 292-3, April 30, 2003.
[23] Positive Technologies Security Advisory, SA2003-0310, April 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ethereal Group[24, 25, 26, 27] ***SuSE releases advisory***[28] ***More updates issued***[29, 30, 31]	**Unix**	**Ethereal 0.8.18**	**Two vulnerabilities exist: a format string vulnerability exists in the SOCKS dissector, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code; and a vulnerability exists in the NTLMSSP dissector, which could let a malicious user execute arbitrary code.**	**Upgrade available at:** **http://www.ethereal.com/distribution/ethereal-0.9.10.tar.gz** **Debian:** **http://security.debian.org/pool/updates/main/e/ethereal/** ***SuSE:*** **ftp://ftp.suse.com/pub/suse** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br/** ***RedHat:*** **ftp://updates.redhat.com** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php**	**Ethereal SOCKS Dissector Format String & NTLMSSP Overflow** **CVE Names: CAN-2003-0081, CAN-2003-0159**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Exploit scripts have been published.**
Francisco Burzi[32]	Unix	PHP-Nuke 6.5 FINAL	Multiple Cross-Site Scripting vulnerabilities exist due to insufficient validation of user input used in an attribute inside a tag, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Multiple PHP-Nuke Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
GKrellM News-ticker[33]	Unix	GKrellM Newsticker 0.3	Two vulnerabilities exist: a vulnerability exists because shell metacharacters are not sanitized from a URI that is supplied by a news feed, which could let a remote malicious user execute arbitrary commands; and a Denial of Service vulnerability exists when a malicious user submits malformed RDF files.	Upgrade available at: http://security.debian.org/pool/updates/main/g/gkrellm-newsticker	Newsticker Malformed Remote Command Execution & RDF Denial of Service CVE Names: CAN-2003-0205, CAN-2003-0206	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.

[24] Georgi Guninski Security Advisory #60, March 8, 2003.
[25] Ethereal Advisory, enpa-sa-00008, March 7, 2003.
[26] Debian Security Advisory, DSA 258-1, March 10, 2003.
[27] Gentoo Linux Security Announcement, 200303-10, March 9, 2003.
[28] SuSE Security Announcement, SuSE-SA:2003:019, March 21, 2003.
[29] Conectiva Linux Security Announcement, CLA-2003:627, April 16, 2003.
[30] Red Hat Security Advisory, RHSA-2003:076-01, April 23, 2003.
[31] Mandrake Linux Security Update Advisory, MDKSA-2003:051, April 25, 2003.
[32] Secunia Security Advisory, April 25, 2003.
[33] Debian Security Advisory, DSA 294-1, April 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GNOME [34] ***Conectiva issues advisory***[35]	**Unix**	**Balsa 2.0.6, 1.2.4, 1.1.7; libesmtp libesmtp 0.8.9, 0.8.4, 0.8.10p1, 0.8.10**	**A buffer overflow vulnerability exists in the read_smtp_response() function, which could let a malicious user execute arbitrary code.**	**Gnome:** **http://balsa.gnome.org/balsa-2.0.10.tar.bz2** **RedHat:** **ftp://updates.redhat.com/** **libesmtp:** **http://www.stafford.uklinux.net/libesmtp/libesmtp-1.0.tar.bz2** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br**	**libesmtp read_smtp_response Buffer Overflow** **CVE Name: CAN-2002-1090**	**High**	**Bug discussed in newsgroups and websites.**
GoldStone Software, Inc.[36]	Multiple	Web Protector 2.	A vulnerability exists due to an encryption weakness, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Web Protector Encryption Weakness	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Gregory DEMAR[37]	Windows, Unix	Coppermine Photo Gallery 1.0 RC3, 1.1 beta 2, 1.1.0	An SQL injection vulnerability exists in the 'displayimage.php' script, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Photo Gallery 'Displayimage.php' SQL Injection	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Gzip.org [38] ***More updates issued***[39, 40,] ***NetBSD issues update***[41, 42] ***RedHat issues advisory***[43]	**Unix**	**zlib 1.1.4**	**A buffer overflow vulnerability exists in the compression library due to insufficient bounds checking of user-supplied data to the gzprintf() function, which could let a malicious user execute arbitrary instructions.**	**OpenPKG:** **http://www.openpkg.org/security/OpenPKG-SA-2003.015-zlib.html** ***SCO:*** **ftp://ftp.sco.com/pub/updates/OpenLinux** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***NetBSD:*** **ftp://ftp.netbsd.org/pub/NetBSD/security/patches/** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br** ***RedHat:*** **ftp://updates.redhat.com**	**Zlib gzprintf() Buffer Overflow** **CVE Name: CAN-2003-0107**	**High**	**Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.**

[34] Red Hat Security Advisory, RHSA-2003:109-03, April 3, 2003.
[35] Conectiva Linux Security Announcement, CLA-2003:630, April 22, 2003.
[36] Bugtraq, April 22, 2003.
[37] SecurityFocus, April 30, 2003
[38] OpenPKG Security Advisory, OpenPKG-SA-2003.015, March 4, 2003.
[39] SCO Security Advisory, CSSA-2003-011.0, March 10, 2003.
[40] Mandrake Linux Security Update Advisory, MDKSA-2003:033, March 18, 2003.
[41] NetBSD Security Advisory, 2003-004, March 26, 2003.
[42] Conectiva Linux Security Announcement, CLA-2003:619, April 7, 2003
[43] Red Hat Security Advisory, RHSA-2003:079-01, April 29, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company [44]	OpenVMS, Unix	Compaq Tru64 5.0a, PK3 (BL17), 5.1a, 5.1a PK4 (BL21), PK3 (BL3), PK2 (BL2), PK1 (BL1), 5.1, 5.1 PK6 (BL20), PK5 (BL19), PK4 (BL18), PK3 (BL17); HP MPE/iX 4.0, 4.5, 5.0, 5.5, 6.0, 6.5, 7.0, 7.5, OpenVMS Secure Web Server 1.1–1, 1.2	A remote Denial of Service vulnerability exists in the NFS daemon due to the way the Cluster Alias/NFS services handle malicious network traffic.	Patch available at: http://ftp.support.compaq.com/patches/public/unix/v5.1b/t64v51bb1-c0007503-18084-es-20030415.tar	TruCluster Alias/NFS Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Hewlett Packard Company [45]	Unix	HP-UX 10.10, 10.16, 10.20, 10.24, 10.26, 10.30, 10.34, 11.04, 11.0, 11.11, 11.20, 11.22	A buffer overflow vulnerability exists in 'rexec' due to a boundary error, which could let a malicious user execute arbitrary code with root privileges.	HP has released a fix for HP-UX 11.00 available at: http://itrc.hp.com/ Users of HP-UX 10.10 systems, as a temporary measure, are advised to download and install libc.1.10.20 on affected systems which is available at: ftp://rexec:rexec@hprc.external.hp.com/ ftp://rexec:rexec@192.170.19.51/	HP-UX RExec Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[44] Hewlett-Packard Company Bulletin, SSRT3533, April 22, 2003.
[45] Davide Del Vecchio Adv#5, April 25, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company [46]	Multiple	JetDirect Firmware, any version	A vulnerability exists because documents are accepted from any source without access control limitations, which could let a remote malicious user cause establish an FTP connection and send arbitrary files to the printer to be printed.	**Workaround:** To disable ftp, Telnet to the JetDirect device and type: ftp-config: 0 When this change is made printing via ftp will no longer function. It will also not be possible to update firmware via ftp. The firmware can be updated using the HP Download Manager or Web Jetadmin.	JetDirect Printers FTP Service File Printing	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Invision Power Services[47]	Windows, Unix	Invision Board 1.0-1.1.1	A vulnerability exists because restricted forum credentials are stored in plaintext that is embedded in cookie data, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Invision Board Plaintext Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
James Theiler[48]	Unix	opt 3.12, 3.13, 3.16, 3.17, 3.18	A buffer overflow vulnerability exists in several Libopt.a error logging functions due to insufficient bounds checking of user-supplied data, which could let a malicious user execute arbitrary code.	Upgrade available at: http://nis-www.lanl.gov/~jt/Software/opt/opt-3.19.tar.gz	Libopt.a Error Logging Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[46] Hewlett-Packard Company Security Bulletin, HPSBMI0304-004, April 22, 2003.
[47] Bugtraq, April 25, 2003.
[48] Secure Network Operations, Inc. Advisory, SRT2003-04-24-1532, April 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
KDE[49, 50, 51] ***More updates issued***[52, 53, 54, 55]	**Unix**	**KDE 2.0-3.1.1**	**A vulnerability exists when specially formatted PDF and PS files are processed due to the way the Ghostscript software is used, which could let a malicious user execute arbitrary commands.**	**KDE:** **http://download.kde.org/stable/3.0.5b/** **Debian:** **http://security.debian.org/pool/updates/main/k/kdegraphics/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***SuSE:*** **ftp://ftp.suse.com/pub/suse** ***Debian:*** **http://security.debian.org/pool/updates/main/k/kdelibs/** **http://security.debian.org/pool/updates/main/k/kdebase/kde**	**KDE Postscript/PDF File Processing** **CVE Name: CAN-2003-0204**	**High**	**Bug discussed in newsgroups and websites.**
Kerio Technologies[56]	Windows	Personal Firewall 2 2.1.4	A vulnerability exists because UDP traffic to and from port 53 is allowed, which could let a remote malicious user bypass firewall filters.	No workaround or patch available at time of publishing.	Personal Firewall Filter Bypass	Medium	Bug discussed in newsgroups and websites.
Kerio Technologies[57]	Windows	Personal Firewall 2 2.1-2.1.4	A buffer overflow vulnerability exists during the administration authentication process, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Personal Firewall Remote Authentication Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Kerio Technologies[58]	Windows	Personal Firewall 2 2.1-2.1.4	A vulnerability exists in the authentication mechanism for remote administration because communication data captured from a valid remote Firewall administration session may be replayed, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Personal Firewall Replay Attack	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[49] KDE Security Advisory, April 9, 2003.
[50] Debian Security Advisory, DSA 284-1, April 12, 2003.
[51] Sorcerer Update Advisory SORCERER2003-04-12, April 12, 2003.
[52] Mandrake Linux Security Update Advisory, MDKSA-2003:049, April 17, 2003.
[53] SuSE Security Announcement, SuSE-SA:2003:0026, April 24, 2003.
[54] Debian Security Advisory, DSA 293-1, April 23, 2003.
[55] Debian Security Advisory, DSA 296-1, April 30, 2003.
[56] Securiteam, April 26, 2003.
[57] Core Security Technologies Advisory, CORE-2003-0305-02, April 28, 2003.
[58] Core Security Technologies Advisory, CORE-2003-0305-02, April 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
LBL[59] *More patches releases*[60, 61] *SuSE releases patch*[62] *More patches released*[63]	Unix	tcpdump 3.4 a6, 3.4, 3.5, 3.5.2, 3.6.2	A vulnerability exists due to a miscalculation in the use of the sizeof operator, which could let a malicious user cause a Denial of Service or execution of arbitrary code.	SCO: ftp://ftp.sco.com/pub/updates/OpenLinux/ Trustix: http://www.trustix.net/pub/Trustix/updates/ *Debian:* http://security.debian.org/pool/updates/main/t/tcpdump/ *Mandrake:* http://www.mandrakesecure.net/en/ftp.php *SuSE:* ftp://ftp.suse.com/pub/suse *RedHat:* ftp://updates.redhat.com	TCPDump Memory Corruption	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
LBL[64, 65, 66, 67, 68] *SuSE releases upgrade*[69] *More patches released*[70, 71]	Unix	tcpdump 3.5.2, 3.6.2, 3.7, 3.7.1	A remote Denial of Service vulnerability exists when maliciously formatted ISAKMP packets are submitted.	Upgrade available at: http://www.tcpdump.org/release/tcpdump-3.7.2.tar.gz Debian: http://security.debian.org/pool/updates/main/t/tcpdump/ OpenPKG: ftp://ftp.openpkg.org/release/1.2/UPD/tcpdump-3.7.1-1.2.1.src.rpm Mandrake: http://www.mandrakesecure.net/en/ftp.php *SuSE:* ftp://ftp.suse.com/pub/suse *Conectiva:* ftp://atualizacoes.conectiva.com.br/ *RedHat:* ftp://updates.redhat.com	TCPDump Malformed ISAKMP Packet Remote Denial of Service CVE Name: CAN-2003-0108	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[59] SCO Security Advisory, CSSA-2002-050.0, November 20, 2002.
[60] Debian Security Advisory, DSA 255-1, February 27, 2003.
[61] Mandrake Linux Security Update Advisory, MDKSA-2003:027, March 3, 2003.
[62] SuSE Security Announcement, SuSE-SA:2003:0015, March 13, 2003.
[63] Red Hat Security Advisory, RHSA-2003:032-01, April 23, 2003.
[64] iDEFENSE Security Advisory, February 27, 2003.
[65] Debian Security Advisory, DSA 255-1, February 27, 2003.
[66] Mandrake Linux Security Update Advisory, MDKSA-2003:027, March 3, 2003.
[67] OpenPKG Security Advisory, OpenPKG-SA-2003.014, March 4, 2003.
[68] Gentoo Linux Security Announcement, 200303-5, March 5, 2003.
[69] SuSE Security Announcement, SuSE-SA:2003:0015. March 13, 2003.
[70] Conectiva Linux Security Announcement, CLA-2003:629, April 22, 2003.
[71] Red Hat Security Advisory, RHSA-2003:032-01, April 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
LBL[72] ***More updates issued***[73, 74]	**Unix**	**tcpdump 3.5.2, 3.6.2, 3.7, 3.7.1**	**A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted RADIUS network packet.**	**Debian:** **http://security.debian.org/pool/updates/main/t/tcpdump/** ***RedHat:*** **ftp://updates.redhat.com/** ***Engarde:*** **http://infocenter.guardiandigital.com/advisories/**	**TCPDump Malformed RADIUS Packet Remote Denial of Service** **CVE Name: CAN-2003-0093**	**Low**	**Bug discussed in newsgroups and websites.**
Linux-atm[75]	Unix	linux-atm les 2.4	A buffer overflow vulnerability exists in the 'les' utility due to insufficient bounds checking of user-supplied input, which could let a malicious user execute arbitrary code with root privileges.	No workaround or patch available at time of publishing.	Linux-ATM 'les' Command Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Macromedia[76]	Windows NT 4.0/2000, XP	ColdFusion Server MX Profes-sional, MX Enterprise, MX Developer, MX 6.0	An information disclosure vulnerability exists in the default installation because an error page returns the installation path, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ColdFusion MX Path Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Matthew Smith[77] ***RedHat issues advisory***[78]	**Unix**	**mICQ 0.4.3, 0.4.6, 0.4.9, 0.4.9.2b, 0.4.9.3, 0.4.9.4,**	**A Denial of Service vulnerability exists when a malicious user submits certain types of ICQ messages that do not contain the required 0xFE separator.**	**Debian:** **http://security.debian.org/pool/updates/main/m/micq/** ***RedHat:*** **ftp://updates.redhat.com**	**mICQ Denial of Service**	**Low**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Microsoft[79]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0, 5.5, SP1&SP2, 6.0, SP1	A Denial of Service vulnerability exists due to an error in the way certain self-referential <OBJECT> definitions are handled in HTML documents.	No workaround or patch available at time of publishing.	Internet Explorer Self-Referential Object Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[72] Debian Security Advisory, DSA 261-1, March 14, 2003.
[73] Red Hat Security Advisory, RHSA-2003:032-01, April 23, 2003.
[74] Guardian Digital Security Advisory, ESA-20030430-014, April 30, 2003.
[75] Securiteam, April 26, 2003.
[76] Network Intelligence India Pvt. Ltd. Advisory, April 26, 2003.
[77] Debian Security Advisory, DSA 211-1, December 13, 2002.
[78] Red Hat Security Advisory, RHSA-2003:118-01, April 24, 2003.
[79] Bugtraq, April 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[80]	Windows 2000	2000 Advanced Server. SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3	A buffer overflow vulnerability exists in the 'regedit.exe' program due to improper bounds checking, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Windows RegEdit.EXE Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[81]	Windows 2000, XP	BizTalk Server 2000 Developer Edition, SP1a, SP2, 2000 Enterprise Edition, SP1a, SP2, 2000 Standard Edition, SP1a, SP2, 2002 Developer Edition, 2002 Enterprise Edition	Two vulnerabilities exist: a buffer overflow vulnerability exists in the HTTP Receiver component due to a boundary error, which could let a remote malicious user cause a Denial or Service or execute arbitrary code *(Note: this vulnerability only affects BizTalk Server 2002);* and a vulnerability exists due to an input validation error in some of the pages used by the DTA (Document Tracking and Administration) web interface, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-016.asp	BizTalk Buffer Overflow & DTA Interface CVE Names: CAN-2003-0117, CAN-2003-0118	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Microsoft[82]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0.1, SP1-SP3, 5.5, 5.5 SP1&2, 6.0, SP1	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in 'URLMON.DLL' due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code; and an input validation vulnerability exists in 'plugin.ocx' due to insufficient checking of parameters, which could let a remote malicious user execute arbitrary script code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-015.asp	Internet Explorer Multiple Vulnerabilities CVE Name: CAN-2003-0113, CAN-2003-0115	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[80] NTBugtraq, April 16, 2003.
[81] Microsoft Security Bulletin, MS03-016, April 30, 2003.
[82] Microsoft Security Bulletin, MS03-015, April 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[83]	Windows 95/98/ME/ NT 4.0/2000, XP	FrontPage 97, 98, 2002, SP1, Internet Explorer 5.0, 5.0.1, SP1-SP3, 5.5, SP1&2, 6.0, SP1, Windows 2000 Advanced Server, SP1-SP3, Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, Windows ME, XP Home, SP1, XP Professional, SP1	A remote Denial of Service vulnerability exists in the 'shlwapi.dll' dynamic link library due to a NULL pointer dereference bug.	No workaround or patch available at time of publishing.	Microsoft Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft[84]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 6.0 SP1	A Denial of Service vulnerability exists when a web page contains a specific CLASSID value and the user attempts to view the page.	No workaround or patch available at time of publishing.	Internet Explorer CLASSID Variant Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[85] ***Microsoft issues bulletin***[86]	**Windows 95/98/ME/ NT 4.0/2000**	**Internet Explorer 5.5, 5.5 SP1&SP2, 6.0, 6.0 SP1**	**A vulnerability exists when the dragDrop() ActiveX method is used, which could let a remote malicious user obtain sensitive information.**	***Frequently asked questions regarding this vulnerability and the patch can be found at:*** **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-015.asp**	**Internet Explorer dragDrop Method** **CVE Name: CAN-2003-0114**	**Medium**	**Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.**

[83] Bugtraq, April 22, 2003.
[84] Bugtraq, April 18, 2003.
[85] Bugtraq, February 3, 2003.
[86] Microsoft Security Bulletin, MS03-015, April 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[87] ***Microsoft issues bulletin***[88]	**Windows 98/ME/NT 4.0/2000**	**Internet Explorer 6.0, 6.0 SP1**	**A vulnerability exists in the showModalDialog and ShowModelessDdialog functions when script code is injected into the style parameters due to improper checks, which could let a remote malicious user execute arbitrary JavaScript and HTML code**	***Frequently asked questions regarding this vulnerability and the patch can be found at:*** **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-015.asp**	**Microsoft Internet Explorer Dialog Style Same Origin Policy Bypass** **CVE Name: CAN-2003-0116**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.** ***Vulnerability has appeared in the press and other public media.***
Microsoft[89]	Windows 95/98/NT 4.0/2000	Outlook Express 5.5, 6.0	A vulnerability exists in the MHTML URL Handler, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the workaround can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-014.asp	Microsoft Outlook Express MHTML URL Handler File Rendering CVE Name: CAN-2002-0980	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. Vulnerability has appeared in the press and other public media.
Microsoft[90]	Windows 95/98/ME/ 2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, Windows 95, 95 SR2, 98, 98SE, ME, XP Home, SP1, XP Professional, SP1	A vulnerability exists in the NTLM Authentication implementation used by the Windows Server Message Block (SMB) protocol and other services in all Windows operating systems, which could let a remote malicious user obtain access to a target user's shared resources.	No workaround or patch available at time of publishing.	Windows SMB NTLM Authentication Interception	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

[87] Bugtraq, December 3, 2002.
[88] Microsoft Security Bulletin, MS03-015, April 23, 2003.
[89] Microsoft Security Bulletin, MS03-014, April 23, 2003.
[90] Securiteam, April 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[91] *Microsoft releases a new bulletin*[92]	Windows 2000	Windows 2000 Terminal Services, Terminal Services SP1-SP3, 2000 Server, Server SP1-SP3, 2000 Professional, Professional SP1-SP3, 2000 Datacenter Server, Datacenter Server SP1-SP3, 2000 Advanced Server, Advanced Server SP1-SP3	A vulnerability exists in the Winlogon NetDDE Agent, which could let a malicious user obtain elevated privileges.	*Frequently asked questions regarding this vulnerability and the patch can be found at:* http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-071.asp	Windows 2000 NetDDE Privilege Escalation	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Microsoft[93] *Proof of Concept exploit released*[94] *Microsoft updates bulletin*[95]	Windows 2000 *Windows NT 4.0*	Windows 2000, ISS 5.0 *Windows NT 4.02, Windows NT 4.0 Terminal Server Edition*	A buffer overflow vulnerability exists in the Windows component used by Web-based Distributed Authoring and Versioning (WebDAV) due to insufficient bounds checking on data, which could let a remote malicious user execute arbitrary code. *Windows NT 4.0 also contains the vulnerability in ntdll.dll, however it does not support WebDAV and therefore the known exploit was not effective against Windows NT 4.0. Microsoft has now released a patch for Windows NT 4.0.*	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-007.asp	Windows 2000 WebDAV Buffer Overflow CVE Name: CAN-2003-0109	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media. *Proof of Concept exploit script has been published.*

[91] Security Advisory 10.06.2002, October 9, 2002.
[92] Microsoft Security Bulletin, MS02-071 V3.0, April 30, 2003.
[93] Microsoft Security Bulletin, MS03-007 V1.1, March 18, 2003.
[94] Bugtraq, March 25, 2003.
[95] Microsoft Security Bulletin, MS03-007 2.1, April 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[96]	Windows XP	Windows XP Home, SP1, XP Professional, SP1	A vulnerability exists when the Service Control Manager (SCM) signals system shutdown and a service has not been able to shutdown properly in the allotted time, which could let a malicious user obtain sensitive information.	Microsoft has stated that the issue will be addressed in Windows Server 2003.	Windows Service Control Manager	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Mike Bobbit[97]	Unix	Album.pl 0.61	A vulnerability exists when alternate configuration files are used, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: http://perl.bobbitt.ca/album/album62.zip	Album.PL Remote Command Execution	**High**	Bug discussed in newsgroups and websites.
mod_auth_any[98]	Unix	mod_auth_any 1.2.2	A vulnerability exists in the mod_auth_any Apache module due to insufficient sanitization of user-supplied arguments, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: http://rhn.redhat.com/	Apache Mod_Auth_Any Remote Command Execution CVE Name: CAN-2003-0084	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
mod_ntlm[99]	Unix	mod_ntlm 0.1-0.4, mod_ntlm2 0.1	Two vulnerabilities exist in the NTLM authentication module; a buffer overflow vulnerability exists in the log() function due to insufficient due to insufficient checking of user-supplied data, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the log() function due to a failure to filter format string characters from user-supplied input provided to an ap_log_rerror() call, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Mod_NTLM Authorization Buffer Overflow & Format String	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Monkey[100]	Unix	Monkey HTTP Daemon 0.4-0.6.1	A buffer overflow vulnerability exists in the PostMethod() procedure due to a boundary error, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://monkeyd.sourceforge.net/get_monkey.php?ver=4	Monkey PostMethod() Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[96] Bugtraq, April 19, 2003.
[97] Securiteam, April 28, 2003.
[98] RedHat Security Advisory, RHSA-2003:114-09, April 28, 2003.
[99] Bugtraq, April 21, 2003.
[100] Securiteam, April 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mozilla[101]	Unix	Bugzilla 2.10, 2.12, 2.14-2.14.5, 2.16-2.16.2, 2.17, 2.17.1, 2.17.3	A vulnerability exists because temporary files are insecurely created, which could let a malicious user corrupt or overwrite files.	Patches available at: http://ftp.mozilla.org/pub/webtools/	Bugzilla Insecure Temporary File Handling	Medium	Bug discussed in newsgroups and websites.
Mozilla[102]	Unix	Bugzilla 2.16-2.17.1, 2.17.3	Several vulnerabilities exist: a vulnerability exists when bug dependency graphs are generated via the GraphViz suite due to insufficient sanitization of HTML, which could let a malicious user execute arbitrary HTML and script code; and multiple Cross-Site Scripting vulnerability exist in the default HTML templates due to insufficient sanitization of user-supplied input, which could let a malicious user execute arbitrary HTML and script code.	Patches available at: http://ftp.mozilla.org/pub/webtools/	Bugzilla Graph HTML Injection & Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
MPCSoft Web[103]	Windows	Guest Book 1.0	Several vulnerabilities exist: a vulnerability exists in the 'insertguest.asp' script due to a failure to filter user-input in the Name, Location, and Comment fields, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because the database file is not secured sufficiently, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	MPCSoftWeb Guest Book HTML Injection & Information Disclosure	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required for the insertguest.asp vulnerability. The information disclosure vulnerability can be exploited via a web browser.

[101] Bugzilla Security Advisory, April 24, 2003.
[102] Bugzilla Security Advisory, April 24, 2003.
[103] Black Tigerz Research Group Advisory, April 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[104]	Windows 2000, Unix	Cisco WebNS 5.0.3, 5.0.0.1.05, 7.1 0.1.02; ISC BIND 9.1-9.1.3, 9.2.0-9.2.2; Microsoft Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Server, 2000 Server	A remote Denial of Service vulnerability exists due to the way some types of DNS requests are handled.	**Cisco:** http://www.cisco.com/tac	Multiple Vender Name Server NXDomain Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Multiple Vendors[105] ***New exploit script published***[106]	**Windows, Unix**	**IBM JDK 1.3.1; Sun JRE (Linux, Solaris, Windows Production Release) 1.3.1-1.3.1_07, 1.4-1.4.0_03, 1.4.1, 1.4.1_01, Sun SDK (Linux, Solaris, Windows Production Release) 1.3.1-1.3.1_07, 1.4-1.4.0_03, 1.4.1, 1.4.1_01**	**A Denial of Service vulnerability exists in several java.util.zip implementations due to insufficient checks to see whether the parameters are NULL values.**	**Upgrade to Sun JDK 1.4.1_02 available at:** **http://java.sun.com/j2se/1.4/**	**Multiple Vendor Java Virtual Machine java.util.zip Null Value Denial of Service**	**Low**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***

[104] Cisco Security Advisory, April 30, 2003.
[105] Bugtraq, March 14, 2003.
[106] Bugtraq, April 29, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts

Multiple Vendors [107, 108]
More vendors release upgrades [109]
More vendors release upgrades [110, 111]
	Unix	Cray UNICOS 6.0, 6.0 E, 6.1, 7.0, 8.0, 8.3, 9.0, 9.0.2.5, 9.2, 9.2.4;
		FreeBSD 4.0- 4.6, 4.7, 5.0, 4.1.1–4.7 Stable & Release;
		GNU glibc 2.1-2.1.3, 2.2-2.2.5, 2.3-2.3.2;
		HP HP-UX 10.20 Series 700 & 800, 10.20, 10.24, 11.04, 11.0, 11.11, 11.20, 11.22;
		IBM AIX 4.3.3, 5.1, 5.2;
		MIT Kerberos 5 1.2-1.2.7;
		OpenAFS 1.0-1.3.2;
		OpenBSD 2.0-3.2;
		SGI IRIX 6.5-6.5.20, 6.5m-6.5.20m, 6.5f-6.5.20f;
		Sun Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86,, 9.0, 9.0_x86
			An integer overflow vulnerability exists in the xdrmem_getbytes() function that is distributed as part of the Sun Microsystems XDR library, which could let a remote malicious user execute arbitrary code.	FreeBSD:
				ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:05/xdr-4.patch
				SCO:
				ftp://ftp.sco.com/pub/updates/OpenLinux/
				MIT:
				http://web.mit.edu/kerberos/www/advisories/2003-003-xdr_patch.txt
				RedHat:
				ftp://updates.redhat.com/
				IBM:
				http://techsupport.services.ibm.com/r
				FreeBSD:
				ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:05/xdr-4.patch
				Debian:
				http://security.debian.org/pool/updates/main/o/opensh-krb5/
				Mandrake:
				http://www.mandrakesecure.net/en/ftp.php
				NetBSD:
				ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-008.txt.asc
				Trustix:
				http://www.trustix.net/pub/Trustix/updates/
				Immunix:
				http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/
				Conectiva:
				ftp://atualizacoes.conectiva.com.br/
					Sun XDR Library xdrmem_getbytes() Integer Overflow
					CVE Name: CAN-2003-0028
						High	Bug discussed in newsgroups and websites.

[107] eEye Security Advisory, AD20030318, March 19, 2003.
[108] CERT® Advisory, CA-2003-10, March 19, 2003.
[109] SecurityFocus, April 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [112, 113, 114]	MacOS X 10.2, Unix	Apache Software Foundation Apache 2.0, 2.0a9, 2.0.28, 2.0.32, 2.0.35-2.0.44; Apple MacOS X Server 10.2-10.2.4; HP Apache-Based Web Server 2.0.43 .04, 2.0.43 .00, 1.0.01.01, 1.0.00.01, 1.0.2 .01	A Denial of Service vulnerability exists due to the way Apache handles excessive amounts of consecutive linefeed characters.	**Apache:** http://www.apache.org/dist/httpd/ **RedHat:** ftp://updates.redhat.com/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Apple:** This issue is addressed in MacOS X Server 10.2.5. This update can be applied via the Software Update pane in System Preferences.	Apache Web Server Linefeed Denial of Service CVE Name: CAN-2003-0132	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit scripts have been published.
Multiple Vendors [115, 116, 117] ***More updates issued*** [118]	**Unix**	**BSD lpr 2000.05.07, 0.48; FreeBSD FreeBSD 2.2-2.2.6; lpr-ppd lpr-ppd 0.72; lprold lprold 3.0.48; OpenBSD OpenBSD 2.0-2.9, 3.0-3.2**	**A buffer overflow vulnerability exists in the 'lpr' printer spooling system, which could let a malicious user execute arbitrary code as root.**	**Debian:** **http://security.debian.org/pool/updates/main/l/lpr/** **SuSE:** **ftp://ftp.suse.com/pub/suse/** **OpenBSD:** **ftp://ftp.openbsd.org/pub/OpenBSD/patches/** ***SGI:*** **http://support.sgi.com/**	**Multiple Vendor LPRM Buffer Overflow** **CVE Name: CAN-2003-0144**	**High**	**Bug discussed in newsgroups and websites. Exploit scripts have been published.**

[110] Immunix Secured OS Security Advisory, IMNX-2003-7+-009-01, April 15, 2003.
[111] Conectiva Linux Security Announcement, CLA-2003:633, April 30, 2003.
[112] Red Hat Security Advisory, RHSA-2003:139-01, April 9, 2003.
[113] Hewlett-Packard Company Security Bulletin, HPSBUX0304-256, April 25, 2003.
[114] Conectiva Linux Security Announcement, CLA-2003:632, April 30, 2003.
[115] SuSE Security Announcement, SuSE-SA:2003:0014, March 13, 2003.
[116] Debian Security Advisory, DSA 267-1, March 24, 2003.
[117] Debian Security Advisory, DSA 275-1, April 2, 2003.
[118] SGI Security Advisory, 20030406-02-P, April 25, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [119, 120, 121, 122] *More vendors release upgrades* [123, 124, 125, 126, 127] *More updates issued*[128, 129, 130]	Unix	OpenPKG Current, OpenPKG 1.1, 1.2; OpenSSL Project OpenSSL 0.9.6, 0.9.6a-0.9.6I, 0.9.7, 0.9.7a	A side-channel attack in the OpenSSL implementation has been published in a recent paper, which could let a remote malicious user obtain the RSA private key of a target server.	OpenPKG: ftp://ftp.openpkg.org/ Trustix: ftp://ftp.trustix.net/pub/Trustix/updates/ Engarde: ftp://ftp.engardelinux.org/pub/engarde/stable/updates/ OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.1/common/024_blinding.patch *Mandrake:* http://www.mandrakesecure.net/en/ftp.php *NetBSD:* ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-007.txt.asc *FreeBSD:* ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:06/openssl.patch *RedHat:* ftp://updates.redhat.com/ *SuSE:* ftp://ftp.suse.com/pub/suse *Conectiva:* ftp://atualizacoes.conectiva.com.br *Debian:* http://security.debian.org/pool/updates/main/o/openssl/open *Hewlett Packard:* http://www.software.hp.com	OpenSSL Timing Attack RSA Private Key Information Disclosure CVE Name: CAN-2003-0147	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

[119] OpenPKG Security Advisory, OpenPKG-SA-2003.019, March 18, 2003.
[120] OpenPKG Security Advisory, OpenPKG-SA-2003.020, March 18, 2003.
[121] Trustix Secure Linux Security Advisory, TSLSA-2003-0010, March 18, 2003.
[122] EnGarde Secure Linux Security Advisory, ESA-20030320-010, March 20, 2003.
[123] Mandrake Linux Security Update Advisory, MDKSA-2003:035, March 25, 2003.
[124] NetBSD Security Advisory 2003-007, 2003-007, March 26, 2003.
[125] FreeBSD Security Advisory, FreeBSD-SA-03:06, March 26, 2003.
[126] Red Hat Security Advisory, RHSA-2003:101-01, April 1, 2003.
[127] SuSE Security Announcement, SuSE-SA:2003:024, April 4, 2003.
[128] Conectiva Linux Security Announcement, CLA-2003:625, April 10, 2003.
[129] Debian Security Advisory, DSA 288-1. April 17, 2003.
[130] Hewlett-Packard Company Security Bulletin, HPSBUX0304-0255, April 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mutt[131, 132] *More vendors release upgrades* [133, 134, 135, 136, 137] *More upgrades released* [138, 139]	Unix	Mutt 1.3.16, 1.3.17, 1.3.22, 1.3.24, 1.3.25, 1.4.0, 1.5.3	A buffer overflow vulnerability exists because remote internationalized folders are not properly handled, which could let a malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.mutt.org/mutt/mutt-1.4.1i.tar.gz OpenPKG: ftp://ftp.openpkg.org/release *Debian:* http://security.debian.org/pool/updates/main/m/mutt *Slackware:* ftp://ftp.slackware.com/pub/slackware/ *Mandrake:* http://www.mandrakesecure.net/en/ftp.php *RedHat:* ftp://updates.redhat.com/ *SuSE:* ftp://ftp.suse.com/pub/suse *Conectiva:* ftp://atualizacoes.conectiva.com.br	Mutt Remote Folder Buffer Overflow CVE Name: CAN-2003-0140	High	Bug discussed in newsgroups and websites.
MySQL AB[140, 141, 142, 143] *RedHat Issues update*[144]	Unix	MySQL 3.23.52-3.23.54	A Denial of Service vulnerability exists due to a double free() pointer bug in the way mysql_change_user() is handled.	MySQL: http://www.mysql.com/downloads/mysql-3.23.html OpenPKG: ftp://ftp.openpkg.org/release Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://www.trustix.net/pub/Trustix/updates/ Engarde: http://ftp.engardelinux.org/pub/engarde/stable/updates/ *RedHat:* ftp://updates.redhat.com	MySQL Double Free Denial of Service CVE Name: CAN-2003-0073	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[131] Core Security Technologies Advisory, CORE-20030304-02, March 20, 2003.
[132] OpenPKG Security Advisory, OpenPKG-SA-2003.025, March 20, 2003.
[133] SuSE Security Announcement, SuSE-SA:2003:020, March 24, 2003.
[134] Debian Security Advisory, DSA 268-1, March 25, 2003.
[135] Slackware Security Advisory, 2003-03-30, March 30, 2003.
[136] Mandrake Linux Security Update Advisory, MDKSA-2003:041, April 1, 2003.
[137] Red Hat Security Advisory, RHSA-2003:109-03, April 3, 2003.
[138] Conectiva Linux Security Announcement, CLA-2003:626, April 14, 2003.
[139] Conectiva Linux Security Announcement, CLA-2003:630, CLA-2003:635 April 30, 2003.
[140] Mandrake Linux Security Update Advisory, MDKSA-2003:013, February 4, 2003.
[141] OpenPKG Security Advisory, OpenPKG-SA-2003.008, January 29, 2003.
[142] Trustix Secure Linux Advisory, TSLSA-2003-0003, February 20, 2003.
[143] EnGarde Secure Linux Security Advisory, ESA-20030220-004, February 20, 2003.
[144] Red Hat Security Advisory, RHSA-2003:093-02, May 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Netscape[145]	Multiple	Navigator 7.0 2	A Cross-Domain Scripting vulnerability exists because Netscape can be fooled into running scripts in a foreign domain, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Navigator Directory Cross-Domain Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Nokia[146]	Multiple	IPSO 3.3, SP1-SP4, 3.3.1, 3.4-3.4.2	A vulnerability exists because some types of requests through Voyager are not properly handled, which could let a remote malicious user obtain sensitive information.	The vendor has stated that a patch is currently in development.	IPSO File Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Northern Solutions[147]	Windows	Xeneo Web Server 2.2.10	A buffer overflow vulnerability exists when a specially crafted HTTP request that contains malicious HTTP header information is submitted, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Xeneo Web Server Undisclosed Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Northern Solutions[148]	Windows	Xeneo Web Server 2.2.9 .0	A remote Denial of Service vulnerability exists when a malicious user submits a specifically crafted HTTP GET request.	No workaround or patch available at time of publishing.	Xeneo Web Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Onecenter[149]	Multiple	ForumOne 4.0	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of data embedded within HTML tags, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	ForumOne Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[145] Bugtraq, April 29, 2003.
[146] SecurityTracker Alert ID, 1006646, April 24, 2003.
[147] SP Research Labs Advisory, x04, April 23, 2003.
[148] Securiteam, April 22, 2003.
[149] Securiteam, April 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
OpenBB Group[150]	Unix	OpenBB 1.0.5, 1.1 .0	Multiple vulnerabilities exist: a vulnerability exists in the 'index.php' script due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary commands; a vulnerability exists in the 'board.php' script due to insufficient validation of user-supplied input, which could let a malicious user execute arbitrary commands; and a vulnerability exists in the 'member.php' script due to insufficient validation of user-supplied input, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	OpenBB Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.

[150] Securiteam, April 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
OpenSSL Project[151, 152, 153, 154, 155] ***More vendors release upgrades***[156, 157] ***More updates issued***[158, 159, 160]	**Unix**	**OpenSSL 0.9.6i, 0.9.6h, 0.9.6g, 0.9.6e, 0.9.6d, 0.9.6c, 0.9.6b, 0.9.6a, 0.9.6, 0.9.7a, 0.9.7**	**A vulnerability exists because the response of vulnerable servers can be abused, which could let a remote malicious user obtain sensitive information.**	**Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **OpenPKG:** **ftp://ftp.openpkg.org/release** **OpenBSD:** **ftp://ftp.openbsd.org/pub/OpenBSD/patches/** **Engarde:** **ftp://ftp.engardelinux.org/pub/engarde/stable/updates/** **NetBSD:** **ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-007.txt.asc** **FreeBSD:** **ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:06/openssl.patch** **OpenPKG:** **http://www.openpkg.org/security.html** ***RedHat:*** **ftp://updates.redhat.com/** ***SuSE:*** **ftp://ftp.suse.com/pub/suse** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br** ***Debian:*** **http://security.debian.org/pool/updates/main/o/openssl/open** ***Hewlett Packard:*** **http://www.software.hp.com**	**OpenSSL Side Channel Leakage** **CVE Name: CAN-2003-0131**	**Medium**	**Bug discussed in newsgroups and websites.**
Opera Software[161]	Windows 95/98/ME/ NT 4.0/2000, XP	Opera Web Browser 6.0 win32- 6.0.5 win32, 7.0 win3- 7.0 3win32, 7.10	A vulnerability exists due to insufficient bounds checking on filename extensions, which could let a remote malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	Opera 6/7 Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[151] EnGarde Secure Linux Security Advisory, ESA-20030320-010, March 20, 2003.
[152] OpenPKG Security Advisory, OpenPKG-SA-2003.026, March 20, 2003.
[153] FreeBSD Security Advisory, FreeBSD-SA-03:06, March 21, 2003.
[154] Mandrake Linux Security Update Advisory, MDKSA-2003:035, March 25, 2003.
[155] NetBSD Security Advisory, 2003-007, March 26, 2003.
[156] Red Hat Security Advisory, RHSA-2003:101-01, April 1, 2003.
[157] SuSE Security Announcement, SuSE-SA:2003:024, April 4, 2003.
[158] Conectiva Linux Security Announcement, CLA-2003:625, April 10, 2003.
[159] Debian Security Advisory, DSA 288-1. April 17, 2003.
[160] Hewlett-Packard Company Security Bulletin, HPSBUX0304-0255, April 24, 2003.
[161] Bugtraq, April 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Opera Software[162]	Windows 95/98/ME/ NT 4.0/2000, XP	Opera Web Browser 7.0 3win32, 7.0 2win32, 7.0 1win32, 7.10	A vulnerability exists in the 'JavaScript Console' which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Opera JavaScript Console Code Execution	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Opera Software[163]	Windows 95/98/ME/ NT 4.0/2000, XP	Opera Web Browser 7.10	A Denial of Service vulnerability exists when a 'news' URL that is of excessive length is processed.	No workaround or patch available at time of publishing.	Opera 7.10 Permanent Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Oracle Corporation[164]	Windows NT 4.0/2000, XP, Unix OpenVMS	Oracle7 7.3.3, 7.3.4, Oracle8 8.0.1-8.0.6, 8.1.5-8.1.7, Oracle8i 8.0 x, 8.0.6.3, 8.0.6, 8.1 x, 8.1.5, 8.1.6, 8.1.7.1, 8.1.7.4, 8.1.7, Oracle9i 9.0, 9.0.1, 9.0.1.2-9.0.1.4, 9.0.2, 9.2.0.1, 9.2.0.2, Oracle9i Release 2 9.2.1, 9.2.2	A buffer overflow vulnerability exists in the 'CREATE DATABASE LINK' query due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	Patches available at: http://metalink.oracle.com/	Oracle Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Oracle Corporation[165]	Windows	Oracle9i 9.0.2	A vulnerability exists in the administration interface due to a failure to encrypt sensitive authentication credentials, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Oracle9iAS Web Cache Administration Plaintext Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[162] Bugtraq, April 28, 2003.
[163] Bugtraq, April 28, 2003.
[164] NGSSoftware Insight Security Research Advisory, NISR29042003, April 29, 2003.
[165] SecurityFocus, April 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
phpSysInfo[166] ***Upgrade now available*** [167]	**Unix**	**phpSysInfo 2.1**	**A file disclosure vulnerability exists because the include path for several template files and language include files can be influenced, which could let a malicious user obtain sensitive information and execute arbitrary code.**	***Upgrade available at:*** **http://cvs.sourceforge.net/cgi-bin/viewcvs.cgi/phpsysinfo/phpsysinfo-dev/index.php.diff?r1=1.56&r2=1.57**	**phpSysInfo File Disclosures**	**Medium/ High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
PoPToP [168] ***Debian issues advisory*** [169]	**Unix**	**PPTP Server 1.0.1, 1.1.2-1.1.4-b2**	**A buffer overflow vulnerability exists due to insufficient sanity checks when referencing user-supplied input used in various calculations, which could let a remote malicious user execute arbitrary code**	**Upgrade available at:** **http://sourceforge.net/project/showfiles.php?group_id=44827** ***Debian:*** **http://security.debian.org/pool/updates/main/p/pptpd**	**PoPToP PPTP Remote Buffer Overflow** **CVE Name; CAN-2003-0213**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***
Qual-comm[170]	Unix	qpopper 4.0 b14, 4.0-4.0.5, 4.0.5 fc2	A vulnerability exists in the 'poppassd' program, which could let a malicious user execute arbitrary commands as root.	No workaround or patch available at time of publishing.	Qpopper Poppassd Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
SAP[171]	Unix	DB 7.3.00, 7.4	A vulnerability exists in the 'instdbmsrv' and 'instlserver' programs, which could let a malicious user obtain elevated privileges.	Fix available at: http://listserv.sap.com/pipermail/sapdb.sources/2003-April/000142.html	SAP Database Development Tools Privilege Escalation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
SAP[172]	Unix	DB 7.3.29, 7.4.3.7 Beta	A vulnerability exists in a binary during installation due to an access control error and a race condition, which could let a malicious user obtain elevated privileges.	Upgrade available at: http://www.sapdb.org/7.4/sap_db_downloads.htm	SAP Database SDBINST Privilege Escalation	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[166] SecurityFocus, April 4, 2003.
[167] SecurityFocus, April 25, 2003.
[168] Bugtraq, April 9, 2003.
[169] Debian Security Advisory, DSA 295-1, April 30, 2003.
[170] INetCop Security Advisory, 2003-0x82-016, April 28, 2003.
[171] Secure Network Operations, Inc. Advisory, SRT2003-04-22-1336, April 22, 2003.
[172] Secunia Security Advisory, April 25, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Script Logic Corporation[173]	Windows NT 4.0/2000, XP	ScriptLogic 4.01	Several vulnerabilities exist: a vulnerability exists because arbitrary registry modifications can be made, which could let an unauthorized remote malicious user obtain administrative privileges; a vulnerability exists because modifications can be made to the configuration of the client workstation, which could let a remote unauthorized malicious user execute arbitrary script code; and a vulnerability exists when ScriptLogic is installed on a host and a logging share is used due to inadequate access controls, which could let a remote malicious user obtain unauthorized administrative access.	Upgrade available at: http://www.scriptlogic.com/common/download-license.asp?product=ScriptLogic&version=4.15&link=/eng/download-locations-sl4.asp	ScriptLogic Arbitrary Registry & Configuration Modifications & Inadequate Access Control	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
SGI[174]	Unix	IRIX 6.5-6.5.19, 6.5.2m-6.5.19m, 6.5.2f-6.5.19f	A vulnerability exists in the LDAP implementation because some attributes from LDAP servers are not handled properly, which could let a remote malicious user obtain unauthorized access.	Patches available at: ftp://patches.sgi.com/support/free/security/patches/6.5.15/patch5063.tar	IRIX Name Service Daemon LDAP Unauthorized Access CVE Name: CAN-2003-0174	Medium	Bug discussed in newsgroups and websites.
Small FTPD[175]	Windows	SmallFTPD 0.99	Several vulnerabilities exist: a remote Denial of Service vulnerability exists when handling malicious login credentials; and a remote Denial of Service vulnerability exists when an excessive quantity of data is submitted as a malicious FTP command argument.	Upgrade available at: http://smallftpd.free.fr/#last	SmallFTPD Login & FTP Command Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Small FTPD[176]	Windows	SmallFTPD 1.0.2	A Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	SmallFTPD Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[173] CERT Vulnerability Note VU#609137, April 30, 2003.
[174] SGI Security Advisory, 20030407-01-P, April 25, 2003.
[175] SecurityFocus, April 30, 2003.
[176] SecurityFocus, April 30, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Snort Project[177, 178] ***More updates issued***[179, 180, 181]	**Unix**	**Snort 1.8-1.8.7, 1.9, 1.9.1; Smooth Wall 2.0 beta 4**	**A buffer overflow vulnerability exists during the reassembly of TCP packets by the stream4 preprocesser, which could let a remote malicious user execute arbitrary code.**	**Snort Project:** **http://www.snort.org/dl/snort-2.0.0.tar.gz** **SmoothWall:** **http://us0.download.smoothwall.org/archive/updates/2.0/b4/2.0b4-mallard-fixes2.tar.gz** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***Engarde:*** **http://infocenter.guardiandigital.com/advisories/** ***Debian:*** **http://security.debian.org/pool/updates/main/s/snort/**	**Snort TCP Packet Reassembly Buffer Overflow** **CVE Name: CAN-2003-0209**	**High**	**Bug discussed in newsgroups and websites.**
Sonic WALL[182]	Multiple	Sonic WALL PRO100, PRO200, PRO300	A Denial of Service vulnerability exists when a malicious user submits an unusually large HTTP POST to the internal interface.	No workaround or patch available at time of publishing.	SonicWALL HTTP POST Denial of Service	Low/**High** **(High if DDoS best practices not in place)**	Bug discussed in newsgroups and websites.
Squirrel Mail[183]	Unix	Squirrel-Mail 1.0.4, 1.0.5, 1.2.0-1.2.10	Multiple Cross-Site Scripting vulnerabilities exist, which could let a malicious user execute arbitrary HTML and script code.	**SquirrelMail:** http://www.squirrelmail.org/download.php **RedHat:** ftp://updates.redhat.com/	Multiple SquirrelMail Cross-Site Scripting CVE Name: CAN-2003-0160	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Stoyan Zhekov[184]	Multiple	PT News 1.6, 1.7-1.7.7	A vulnerability exists in the 'news.inc' file due to an authentication error, which could let an unauthorized remote malicious user obtain access to administrative functions.	Upgrade available at: http://www.openbg.net/ptsite/download/	PT News Unauthorized Administrative Access	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[177] NIPC/DHS Advisory 03-018, April 17, 2003.
[178] CERT Advisory, CA-2003-13, April 17, 2003.
[179] Mandrake Linux Security Update Advisory, MDKSA-2003:052, April 28, 2003.
[180] Guardian Digital Security Advisory, ESA-20030430-013, April 30, 2003.
[181] Debian Security Advisory, DSA 297-1, May 1, 2003.
[182] Bugtraq, April 25, 2003.
[183] Red Hat Security Advisory, RHSA-2003:112-01, April 24, 2003.
[184] SecurityTracker Alert ID, 1006615, April 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-Systems, Inc.[185] ***Sun issues patch***[186]	**Unix**	**Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0 8.0_x86, 9.0**	**A vulnerability exists in the wall application, which could let a malicious user send spoofed messages.**	***Patch available at:*** **http://sunsolve.sun.com**	**Solaris Wall Spoofed Message**	**Medium**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
Sun Micro-systems, Inc.[187]	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	A Denial of Service vulnerability exists in the rpcinfo(1M) command.	Patches available at: http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=105402&rev=42	Solaris Rpcinfo Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[188]	Unix	Solaris 8.0, 8.0_x86	A Denial of Service vulnerability exists in the lofiadm(1M) command.	Patches available at: http://sunsolve.sun.com Patch 114163-01, Patch 114162-01	Solaris Lofiadm Kernel Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[189]	Unix	Sun Ray Server Software 1.2, 1.3	A vulnerability exists because the quick removal, reinsertion and removal of a Smartcard may cause the login session to remain connected to the DTU even after the card has been removed.	Workaround available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F53922	Sun Ray Smart Card Removal Session Logout Failure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
The XMB Group[190]	Windows, Unix	Forum 1.8	A vulnerability exists in the 'Members.PHP' script due to insufficient sanitization of user-supplied data, which could let a remote malicious retrieve password hashes including the administrator.	Upgrade available at: http://www.xmbforum.com/download/	XMB Forum Members.PHP SQL Injection	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Tridion[191]	Multiple	Tridion R5 SP2	An information disclosure vulnerability exists because sensitive information that is embedded in certain XML configuration files is stored on the system, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Tridion R5 Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[185] Bugtraq, January 3, 2003.
[186] Sun(sm) Alert Notification, 51980, April 28, 2003.
[187] Sun(sm) Alert Notification, 50922, April 28, 2003.
[188] Sun(sm) Alert Notification, 54100, April 28, 2003.
[189] Sun(sm) Alert Notification, 53922, April 28, 2003.
[190] Binary Bugs Advisory, BB-2003-1, April 22, 2003.
[191] SecurityFocus, April 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Truelogik[192]	Windows, Unix	Truegalerie 1.0	Two vulnerabilities exist: a vulnerability exists in the 'verif_admin.php' and 'check_admin.php' administration scripts due to insufficient sanitization of some URI values, which could let a remote malicious user obtain administrative privileges; and a vulnerability exists in the 'upload.php' script, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Truegalerie Unauthorized Administrative Access & Information Disclosure	Medium/ **High** **(High if administrative access can be obtained)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Twilight Utilities[193] ***Exploit scripts have been published***[194]	**Windows 2000, XP**	**TW_Web Server 1.0**	**A remote Denial of Service vulnerability exists when a malicious user submits an excessive amount of data as part of a HTTP GET request. Execution of arbitrary code may also be possible.**	**No workaround or patch available at time of publishing.**	**TW-Web Server Denial of Service**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.** ***Exploit scripts have been published.*** **Vulnerability has appeared in the press and other public media.**
Working Resources Inc.[195]	Windows 94/98/ME/ NT 4.0/2000, XP	BadBlue Enterprise Edition 1.5, 1.5.6 Beta, 1.6 Beta, 1.7, 1.7.2, 1.7.3, 1.7.4, 2.15, Personal Edition 1.5.6 Beta, 1.6 Beta, 1.7, 1.7.2, 1.7.3, 1.7.4, 2.15	An input validation vulnerability exists in the 'ext.dll' component, which could let an unauthorized remote malicious user execute arbitrary administrative actions.	Upgrade available at: http://www.badblue.com/down.htm	BadBlue 'ext.dll' Remote Command Execution	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Xinetd[196]	Unix	Xinetd 2.3-2.3.10	A remote Denial of Service vulnerability exists in the 'sve_request' function when connection attempts to some services are rejected.	Upgrade available at: http://www.xinetd.org/xinetd-2.3.11.tar.gz	Xinetd Remote Denial of Service CVE Name: CAN-2003-0211	**Low**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[192] Secunia Security Advisory, April 29, 2003.
[193] SP Research Labs Advisory x02, April 15, 2003.
[194] SecurityFocus, April 21, 2003.
[195] Secunia Security Advisory, April 21, 2003.
[196] Bugtraq, April 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Xoops[197]	Windows, Unix	Xoops 1.3.5-1.3.9, 2.0, 2.0.1	A vulnerability exists in the in 'MytextSanitizer' function due to insufficient filtering of user-supplied HTML and script code, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.xoops.org/modules/mydownloads/viewcat.php?cid=16	Xoops MyText Sanitizer Arbitrary Code	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
YaBB SE[198]	Windows, Unix	YaBB SE 1.1.3, 1.4.1, 1.5.1 RC1, 1.5 .0, 1.5.1	A vulnerability exists in the '$language' variable due to an input validation error, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: https://sourceforge.net/project/showfiles.php?group_id=57105&release_id=154462	YaBB SE '$language' Variable	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between April 16 and April 30, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 36 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
April 30, 2003	0x82-Local.Qp0ppa55d.c	Script that exploits the Qpopper Poppassd Command Execution vulnerability.
April 30, 2003	Apache-massacre.c	Script that exploits the Apache Web Server Linefeed Denial of Service vulnerability.

[197] NTBugtraq, April 25, 2003.
[198] Next Generation Security Technologies Security Advisory, NGSEC-2003-5, April 22, 2003.

Date of Script (Reverse Chronological Order)	Script name	Script Description
April 30, 2003	Bysin.c	Script that exploits the Remote Crackaddr() vulnerability.
April 30, 2003	Bysin2.c	Script that exploits the Sendmail Address Prescan Buffer Overflow vulnerability.
April 30, 2003	Getdatang.tar.gz	A sniffer made with libpcap that supports multiple protocols like TCP, UDP, ICMP, IGMP, etc.
April 30, 2003	Injectso-0.2.1.tar.gz	A tool that can be used to inject shared libraries into running processes on Linux (x86/IA32 and Sparc) and Solaris (Sparc). It also provides routines that can be used by injected libraries to easily modify the behavior of the host process by intercepting library function calls.
April 30, 2003	Msqlfast.c	A high-speed brute-force password cracker for MySQL hashed passwords that can break an 8-character password containing any printable ASCII characters in a matter of hours.
April 30, 2003	Poptop-sane.c	Script that exploits the PoPToP PPTP Remote Buffer Overflow vulnerability.
April 30, 2003	Th-apachedos.c	Script that exploits the Apache Web Server Linefeed Denial of Service vulnerability.
April 29, 2003	0x333hate.c	Samba 2.2.x Remote root exploit script.
April 29, 2003	Bug-exploit.tar.bz2	A utility designed to go through a list of setuid and setgid files that will assist a coder in figuring out whether or not a buffer overflow exists in the command line arguments fed to the binary.
April 29, 2003	Crash.cfm	Exploit for the Java Virtual Machine java.util.zip Null Value Denial of Service vulnerability.
April 29, 2003	Nagini.c	A TCP packetlogger/sniffer for Linux which includes background logging.
April 29, 2003	THCunREAL_V0.2.ZIP	Updated version of the remote root exploit for RealServer 8 on several Windows platforms.
April 28, 2003	**Ftpbanex.pl**	**Perl script that exploits the 3D-FTP Client Buffer Overflow vulnerability.**
April 28, 2003	**Kerio-overflow.py**	**Script that exploits the Personal Firewall Remote Authentication Buffer Overflow vulnerability.**
April 27, 2003	Xrunas11eval.zip	A tool that allows administrators to run commands on remote computers under the context of a specified user account without the use of the Schedule service. If XRunAs is used in conjunction with a domain account, commands that are run will be able to access network resources given that the domain account used to run the command has access to the network resource.
April 24, 2003	**Les-exploit.c**	**Script that exploits the Linux-ATM 'les' Command Buffer Overflow vulnerability.**
April 23, 2003	Nmap-3.20_statistics-1.diff	The Nmap 3.20 Statistics Patch adds the -c switch which guesses how much longer the scan will take, shows how many ports have been tested, resent, and the ports per second rate.
April 23, 2003	Osxds.c	Script that exploits the MacOS X Directory Service Denial of Service vulnerability.
April 23, 2003	P7snort191.sh	Script that exploits the Snort TCP Packet Reassembly Buffer Overflow vulnerability.
April 23, 2003	**Sp-xeneo2.c**	**Script that exploits the Xeneo Web Server Undisclosed Buffer Overflow vulnerability.**
April 22, 2003	Envpaper.pdf	Radical Environments part I is a paper that compiles various stack related tips and tricks and discusses how an exploit without nops works.
April 22, 2003	Exmb.c	Script that exploits the XMB Forum Members.PHP SQL Injection vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
April 22, 2003	Netric-RE-partII.pdf	Radical Environments part II is a paper continues where part one left off, detailing a technique in writing 0 bytes when exploiting a local buffer overflow using a non-executable stack with the heap being stored in memory at a virtual address containing a \x00 byte.
April 22, 2003	**Procrack.pl**	**Perl script that exploits the Web Protector Encryption Weakness vulnerability.**
April 21, 2003	Arb-scan-0.5.0.tar.gz	A remote banner scanner, written in Bash and Perl that currently supports ftpd, sshd, smtpd, domain, finger, httpd, pop2, pop3 and imapd banner checks.
April 21, 2003	Fmtstring.txt	Detailed paper that describe format string vulnerabilities and how to exploit them.
April 21, 2003	Kripp-0.2.tar.gz	A simple and lightweight network passwords sniffer written in Perl, which uses tcpdump to intercept traffic.
April 21, 2003	Lkl-0.0.4.tar.gz	A userspace keylogger that runs under linux x86/architecture and logs everything which passes through the hardware keyboard port (0x60). Keycode to ASCII translation is supported.
April 21, 2003	Monkey-nuke.pl	Perl script that exploits the Monkey PostMethod() Buffer Overflow vulnerability.
April 21, 2003	**Sp-urfuqed.pl**	**Perl script that exploit the TW-Web Server Denial of Service vulnerability.**
April 21, 2003	Sp-xeneo.pl	Perl script that exploits the Xeneo Web Server Remote Denial of Service vulnerability.
April 21, 2003	**Ss-dos.c**	**Script that exploit the TW-Web Server Denial of Service vulnerability.**
April 20, 2003	**Backrush.patch**	**Exploit for the Windows SMB NTLM Authentication Interception vulnerability.**
April 16, 2003	**TrapReg.c**	**Script that exploits the Windows RegEdit.EXE Buffer Overflow vulnerability.**

Trends

- According to new research, nearly three-quarters of malicious connections to wireless networks are used for sending spam. A survey found that almost a quarter of unauthorized connections to the wireless Lans were intentional, and 71 per cent of those were used to send emails.
- **The Department of Homeland Security (DHS), Information Analysis and Infrastructure Protection (IAIP) has issued an advisory to heighten awareness of a recently discovered Snort(TM) vulnerability, a heap overflow in the Snort "stream4" preprocessor (CAN-2003-0029). For more information see 'Bugs, Holes, & Patches Table (CyberNotes 2003-08) and DHS/IAIP Advisory 03-018, located at: http://www.nipc.gov/warnings/advisories/2003/03-018.htm**
- **The number of security events detected by companies in the first quarter of 2003 jumped nearly 84 percent over the preceding three months. The increase in events, which can include minor probes for holes in network security as well as major attacks, stems mainly from an increase in worms and automated attack software.**
- Over the past few weeks, their have been an increased number of reports of intruder activity involving the exploitation of Null (i.e., non-existent) or weak Administrator passwords on Server Message Block (SMB) file shares used on systems running Windows 2000 or Windows XP. This activity has resulted in the successful compromise of thousands of systems, with home broadband users' systems being a prime target. Recent examples of such activity are the attack tools known as W32/Deloder, GT-bot, sdbot, and W32/Slackor. For more information, see CERT® Advisory CA-2003-08, located at: http://www.cert.org/advisories/CA-2003-08.html.

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Klez	Worm	Stable	January 2002
2	W32/Yaha	Worm	Stable	February 2002
3	W32/Sobig	Worm	Stable	January 2003
4	W32/Lovegate	Virus	New to table	February 2003
5	Elkern	File Infector	Slight Increase	October 2001
6	JS/NoClose	Trojan	Stable	May 2002
7	W32/Bugbear	Worm	Slight Decrease	September 2002
8	Funlove	File	Stable	November 1999
9	I-Worm.Sircam	Worm	Return to table	July 2001
10	W32/SQLSlammer	Worm	Slight Decrease	January 2003

Note: Virus reporting may be weeks behind the first discovery of infection. A total 202 distinct viruses are currently considered "in the wild" by anti-virus experts, with another 319 viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

I-Worm.Win32.Fasong (Internet Virus): This is a worm that spreads via local area networks. The worm itself is a Windows PE EXE file about 170KB in length and is written in Delphi. The worm has a Trojan routine. While installing, the Fasong worm copies itself to randomly selected directories on randomly selected drives, and using randomly selected EXE names, for example:

- GMLKU.EXE
- TKXMLIB.EXE
- LUFV.EXE

The worm registers these files in the system registry auto-run key.

I-Worm.Yanker (Internet Worm): This is a very dangerous multicomponent worm-virus that spreads through via the Internet as an RAR archive attached to infected e-mails. Infected e-mails contain:

- Subject: Hi,my new webpage ;o)
- Attachment name: webpage.rar

The RAR archive contains the file webpage.htm and a subcatalog named images where the main components of this virus are stored.

VBS.Alphae@mm (Visual Basic Script Worm): This is a worm that spreads by e-mail that has the following characteristics:

- Subject: One Year Later>WTC
- Attachment: EuroAlph@.html.scr.vbs

VBS.Alphae@mm drops numerous malicious files and modifies a system's configuration. This worm also uses mIRC to gain unauthorized access to your computer.

VBS.Alphae.B@mm (Visual Basic Script Worm): This is a worm that spreads by e-mail, which has the following characteristics:

- Subject: YOUR ACCOUNT IS A NIGHTMARE ?
- Attachments: Sys32.Dll.vbs

VBS.Alphae.B@mm modifies the system's configuration and performs annoying actions.

VBS.Annod.C (Visual Basic Script Virus): This is a virus that overwrites Visual Basic (VB) scripts. It is a minor variant of VBS.Annod. VBS.Annod.C displays music-related messages in Spanish and modifies the system settings to launch random programs when you start Windows.

VBS.Terrosist (Alias: VBS/Terrosist.ow) (Visual Basic Script Virus): This is a Visual Basic (VB) Script virus that infects HTML files. It targets files that have the extensions .htt, .htm, .html, .asp, .php, or .jspin.

W32.Boa.Worm (Win32 Worm): This is a mass-mailing worm. It uses its own SMTP engine to spread itself by e-mail. The contents of the e-mail message will vary; however, the size of the attachment contained in the e-mail will be 81,920 bytes. It is written in the Visual Basic programming language. When W32.Boa.Worm runs, it copies itself to %Windir%\System\Msnet.exe and adds the registry value, “MSNET"="%windir%\System\msnet.exe,” to the registry keys:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

so that the worm runs when you start Windows.

W32/Cailont-A (Alias: W32.Nolor@mm, W32/Lovelorn@MM, WORM_LOVELORN.A, Win32.Lovelorn.A, I-Worm.Lovelorn, W32/Lovelorn.dr) (Win32 Worm): This is an Internet worm which sends itself out by e-mail. It creates seven files in your system folder. The files explorer.exe, kernel32.exe, netdll.dll, and serscg.dll are copies of the worm. The file setup.htm is a web page containing a Visual Basic Script that creates and launches the worm. The files Netsn.dll and Bsbk.dll are raw base64-encoded copies of the worm and script files (these files are harmless on their own and can be deleted). W32/Cailont-A adds the value, “explorer = "\SYSTEM\FOLDER\explorer.exe," to the registry key:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

This means that the worm will run automatically every time you start your computer. W32/Cailont-A sends e-mails with the various subjects and message text. W32/Cailont-A names its attachment:

- xxx.KISS.OK.EXE or xxx.HTM (where xxx varies from e-mail to e-mail.)

W32/Coronex-A (Aliases: I-Worm.Coronex.a, W32/Coronex.worm, Win32/Sars.A, W32.Coronex@mm, WORM_CORONEX.A, Win32.Coronex.A) (Win32 Worm): This is an Internet worm which e-mails itself to every contact in the Windows address book. The e-mail characteristics vary depending upon the current day of the week. When first run, the worm displays a message box with the text "SARS Virus, corona virus,” copies itself to the Windows folder as Corona.exe and creates the following registry entry so that corona.exe is run automatically each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\PC-Config32 = %WINDOWS%\corona.exe -A

The worm copies itself to the C:\My Downloads folder using 1 of the 24 filenames depending upon the current hour of the day. When run with a -A command line switch (i.e. on startup), the worm runs continuously in the background and e-mails itself when the time is 1 minute past any hour. The worm also changes the start page for Microsoft Internet Explorer by setting the registry entry:

- HKCU\Software\Microsoft\Internet Explorer\Main\Start Page = http://www.who.int/csr/don/2003_04_19/en

W32/Coronex.worm.b (Alias: I-Worm.Coronex.b) (Win32 Worm): This is a mass-mailing worm that simply spreads via e-mail. It does not contain a destructive payload. The worm sends itself to all addresses in the Windows address book. It arrives as an e-mail attachment. When the attachment is executed, the worm drops a copy of itself in the %WINDIR% directory and displays a message box. It creates a key to run itself during startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "PC-Config32" = C:\%WINDIR%\virus.exe -A

and changes the default browser start page:

- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main "Start Page" = http://www.bitdefender.com

It looks for "C:\My Downloads" and drops a copy of itself there using one of randomly chosen filenames. W32/Coronex.worm.b mails itself to addresses listed in the Windows address book. The worm uses its own SMTP engine to construct the aforementioned messages.

W32.HLLW.Deborms.C (Alias: Worm.Win32.Deborm.q) (Win32 Worm): This is a variant of W32.HLLW.Deborms that attempts to spread through the local network. The worm drops and runs Backdoor.Sdbot and Backdoor.Litmus.

W32.HLLW.Donk (Win32 Worm): This is a worm that spreads through network shares, opening up numerous TCP ports in the process. This worm also has backdoor capabilities that give a malicious user access to your computer.

W32.HLLW.Kefy (Win32 Worm): This is an encrypted worm that attempts to spread itself through the KaZaA, KaZaA Lite, KMD, Morpheus, eDonkey2000, Limewire, Bearshare, iMesh, Overnet, Applejuice, Gnucleus, Grokster, Gnotella, Shareaza, Neomodus, Rapigator, WinMX, and Swapnut file-sharing networks, as well as ICQ. The worm attempts to terminate the processes of various antivirus and security programs. W32.HLLW.Kefy also attempts to copy itself to the root folder of all the drives. This threat is written in the Microsoft Visual Basic programming language.

W32/Holar.g@mm (Win32 Worm): This variant is very similar to previous variants. It is intended to propagate via e-mail and sharing itself over P2P networks. However in testing the worm proved to be buggy and at the time of writing, replication has not been observed (nor successful installation on the victim machine). The worm consists of a 3-file sandwich:

- DROPPER COMPONENT | PROPAGATION COMPONENT | SMTP LIBRARY

The dropper component is intended to drop and run the other components:

- Propagation component: 42,091 bytes
- SMTP library: 15,417 bytes

Strings within the dropper and propagation components suggest the worm is intended to arrive in a message with various subject lines and message bodies.

W32/Jeefo (Win32 Virus): This is a parasitic 32-bit file infecting virus that infects Windows PE files on the victim machine. When an infected file is run on the victim machine, the file SVCHOST.EXE (36,352 bytes) is dropped in %WinDir%. The file is set with the system attribute set. On Windows 9x machines, the following Registry key is added to hook system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices "PowerManager" = %WinDir%\SVCHOST.EXE

On Windows NT/2000/XP machines, the dropped file is installed as a service, with the following characteristics:

- Description: Manages the power save features of the computer

- Display Name: Power Manager
- Start Type: Automatic
- Account: Local system

Once running in memory, the virus periodically attempts to infect PE files on the victim machine.

W32.Jits (Alias: W32.HLLW.VB.A) (Win32 Worm): This is a worm that copies itself as the following files:

- C:\Tits.exe
- C:\Windows\Tits.exe
- C:\Windows\Start Menu\Programs\Startup\Tits.exe
- A:\Tits.exe

It is written in Microsoft Visual Basic, version 6.

W32/Kullan-A (Aliases: W32.HLLW.Kullan, TROJ_TAMPONAI.A, Worm.Win32.Kullan, W32/Sory.worm) (Win32 Worm): This is a complex worm with backdoor functionality that targets available network shared resources. When executed the worm copies itself to the Windows system folder with the filename Services.exe and sets the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  or
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\load
- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\run

and adds the full path to Services.exe to:

- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\shell
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\shell

Running as a background process the worm uses the "net view" command to be able to drop a copy of itself to the Start Menu folder of the available computer using the computer name as a filename. As a backdoor, the worm provides access to confidential information such as OS type, keystroke logs and e-mail details. W32/Kullan-A may also change the Win.ini and System.ini files to make sure the worm will be executed at the next restart.

W32.Kwbot.G.Worm (Alias: Worm.P2P.Tanked.a) (Win32 Worm): This variant attempts to spread itself through file-sharing networks. This worm drops and runs Backdoor.Assasin.F and attempts to disguise itself as an RAR self-extractor. The existence of the file Net_32.exe is an indication of a possible infection.

W32.Sphit (Win32 Worm): This is a worm that copies itself to network folders in which users have access. The existence of the file Dllexe32.exe is an indication of a possible infection. When W32.Sphit is executed, it copies itself as:

- %System%\Dllexe32.exe
- %System%\Dllfolder32.exe

and creates the registry key:

- HKEY_CLASSES_ROOT\xxexile\shell\open\ddeexec

with the string value, “(Default)"="%System%\dllexe32.exe %1.” The worm also modifies the (Default) value of the registry key:

- HKEY_CLASSES_ROOT\Folder\shell\open\command

from, “%Windows%\Explorer.exe /idlist, %I, %L,” to, “%System%\dllfloder32.exe explorer.exe /idlist, %I, %L.” The worm modifies the (Default) value of the registry key:

- HKEY_CLASSES_ROOT\Folder\shell\open\ddeexec

from, [ViewFolder("%l", %I, %S)], to, <none>. When you access any shared folders on the network, the worm copies itself to that folder as <folder name>+<first character of the folder name>.exe.

W32.Yourde (Win32 Virus): W32.Yourde infects files that are opened and saved in the full version of Adobe Acrobat v5.0.5 only. This virus does not work in Acrobat Reader and does not perform any other actions. A patch is available from Adobe Systems, Inc. which addresses this vulnerability at: http://www.adobe.com/support/downloads/detail.jsp?ftpID=2121. W32.Yourde works by exploiting a vulnerability in the JavaScript parser, which exists in Adobe Acrobat v5.0.5. This vulnerability allows JavaScript code to place files in your Plug-ins folder. When an infected PDF file is opened, some JavaScript code in the file will execute and place the file, Death.api, into the Acrobat plug-ins folder (usually C:\Program Files\Adobe\Acrobat 5.0\Acrobat\Plug_ins) and place the file, Evil.fdf, into the root of the C drive. The Death.api file contains the virus replication code and the Evil.fdf file contains the JavaScript code, which launches the virus from the infected files. When Acrobat is restarted, the plug-in will be loaded and the virus will be activated. When the virus activates, it will add the Death.api and Evil.fdf files to any existing PDF file, which is opened and then saved. The virus does not affect the files that are not saved and does not affect the newly created files. In addition, when you edit an infected file, the virus will re-infect the file when the file is saved.

W95.Tenrobot.B (Word 95 Macro Virus): This is a memory-resident, file-appender virus, which is a variant of W95.Tenrobot. It only infects files when it is executed on a Windows 95/98/ME system. W95.Tenrobot.B also attempts to give a malicious user unauthorized access to an infected computer through IRC.

Win32.Spreder (Win32 Virus): This is a nonmemory resident parasitic Win32 virus. It infects .EXE files that have sizes ranging from 100KB to 10MB. The virus itself is a Windows PE EXE file written in Microsoft Visual C++. The virus size is about 60KB, but during the infecting process the size increases by about 410KB. The virus looks for victim EXE files in the KaZaA (file sharing network) download directory (if there is one).If KaZaA is not installed the virus fails to infect any files.

WORM_AGOBOT.F (Aliases: BDS/Agobot.015.F, W32/Gaobot.worm, Worm/Agobot, Win32.Agobot.C) (Win32 Worm): This worm propagates via the KaZaA peer-to-peer file-sharing network and via network shared drives. It attempts to connect to an Internet Relay Chat (IRC) server and act as a bot program that can be used to launch a Denial of Service (DoS)attack against other users. This worm is designed to have backdoor server capabilities that allow remote users to access and manipulate infected systems. This worm runs on Windows 95, 98, NT, 2000, ME, and XP.

Worm/Halfint (Peer-2-Peer Worm): This is an Internet P2P worm that spreads through the use of file-sharing programs. If executed, it copies itself with various filenames to 'C:\My Shared Folder.'

Worm/Opex (Alias: Worm.P2P.Opex) (Peer-2-Peer Network Worm): This is a P2P network worm that spreads through various file-sharing programs such as KaZaA, Morpheus, EDonkey2000. If executed, the worm copies itself in the \windows directory under the filenames:

- C:\Windows\Winstart.exe
- C:\Windows\Sysboot.exe

It will then copy itself to the root of C:\ under:

- C:\Hardcore Sex Scene 1 of 2.exe
- C:\Cool Game.exe

So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "WinStart"="C:\\WINDOWSWinStart.exe"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices "SysBoot"="C:\\WINDOWS\\SYSTEMSysBoot.exe"

WORM_XMS.A (Alias: XMS.A) (Internet Worm): This malware propagates via the KaZaA Peer to Peer Network. It drops a copy of itself named XMS32.EXE in the Windows System directory and, if KaZaA is installed in the compromised machine, it drops multiple copies of itself in a created folder and modifies the Registry so that this folder is shared in the KaZaA Network. It also drops and executes a backdoor malware that Trend Micro detects as BKDR_RAMDAM.A. It runs on Windows 95, 98, NT, 2000, ME, and XP.

X97M.Suhd@mm (Excel 97 Macro Worm): This is an intended worm that attempts to spread using Microsoft Outlook. It copies itself to the Microsoft Excel Startup folder and changes various security settings in the registry.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
AdwareDropper-A	A	CyberNotes-2003-04
AIM-Canbot	N/A	CyberNotes-2003-07
AprilNice	N/A	CyberNotes-2003-08
Backdoor.Acidoor	N/A	CyberNotes-2003-05
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Assasin.F	**F**	**Current Issue**
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	C	CyberNotes-2003-05
Backdoor.Beasty.D	D	CyberNotes-2003-06
Backdoor.Beasty.E	E	CyberNotes-2003-06
Backdoor.Bigfoot	**N/A**	**Current Issue**
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	N/A	CyberNotes-2003-06
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Delf.F	F	CyberNotes-2003-07
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.Dvldr	N/A	CyberNotes-2003-06
Backdoor.EggDrop	N/A	CyberNotes-2003-08
Backdoor.Fluxay	N/A	CyberNotes-2003-07
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.FTP_Ana.C	C	CyberNotes-2003-07
Backdoor.FTP_Ana.D	D	CyberNotes-2003-08
Backdoor.Graybird	N/A	CyberNotes-2003-07
Backdoor.Graybird.B	B	CyberNotes-2003-08
Backdoor.Graybird.C	C	CyberNotes-2003-08
Backdoor.HackDefender	N/A	CyberNotes-2003-06
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04

Trojan	Version	CyberNotes Issue #
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.Kaitex.D	**D**	**Current Issue**
Backdoor.Kalasbot	**N/A**	**Current Issue**
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.Kol	N/A	CyberNotes-2003-06
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.Litmus.203.c	**c**	**Current Issue**
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Longnu	N/A	CyberNotes-2003-06
Backdoor.Marotob	N/A	CyberNotes-2003-06
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.Monator	N/A	CyberNotes-2003-08
Backdoor.MSNCorrupt	N/A	CyberNotes-2003-06
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixDDoS	N/A	CyberNotes-2003-07
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.OptixPro.12.b	12.b	CyberNotes-2003-07
Backdoor.OptixPro.13	**13**	**Current Issue**
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.Pointex	**N/A**	**Current Issue**
Backdoor.Pointex.B	**B**	**Current Issue**
Backdoor.PSpider.310	310	CyberNotes-2003-05
Backdoor.Queen	N/A	CyberNotes-2003-06
Backdoor.Ratega	**N/A**	**Current Issue**
Backdoor.Recerv	**N/A**	**Current Issue**
Backdoor.Redkod	N/A	CyberNotes-2003-05
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.Rsbot	N/A	CyberNotes-2003-07
Backdoor.SchoolBus.B	B	CyberNotes-2003-04
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Sdbot.E	E	CyberNotes-2003-06
Backdoor.Sdbot.F	F	CyberNotes-2003-07
Backdoor.Sdbot.G	G	CyberNotes-2003-08

Trojan	Version	CyberNotes Issue #
Backdoor.Sdbot.H	**H**	**Current Issue**
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Simali	**N/A**	**Current Issue**
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	N/A	CyberNotes-2003-06
Backdoor.SubSari.15	15	CyberNotes-2003-05
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
Backdoor.Syskbot	N/A	CyberNotes-2003-08
Backdoor.SysXXX	N/A	CyberNotes-2003-06
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Tankedoor	N/A	CyberNotes-2003-07
Backdoor.Trynoma	N/A	CyberNotes-2003-08
Backdoor.Turkojan	N/A	CyberNotes-2003-07
Backdoor.Udps.10	10	CyberNotes-2003-03
Backdoor.Unifida	N/A	CyberNotes-2003-05
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.XTS	N/A	CyberNotes-2003-08
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zombam	N/A	CyberNotes-2003-08
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	ARR	CyberNotes-2003-06
Backdoor-ARU	ARU	CyberNotes-2003-06
BackDoor-ARX	ARX	CyberNotes-2003-06
BackDoor-ARY	ARY	CyberNotes-2003-06
BackDoor-ASD	ASD	CyberNotes-2003-07
BackDoor-ASL	ASL	CyberNotes-2003-07
BackDoor-ASW	ASW	CyberNotes-2003-08
BackDoor-ATG	**ATG**	**Current Issue**
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/Ciadoor.10	10	CyberNotes-2003-07
BDS/Evilbot.A	**A**	**Current Issue**
BDS/Evolut	N/A	CyberNotes-2003-03
Daysun	N/A	CyberNotes-2003-06
DDoS-Stinkbot	N/A	CyberNotes-2003-08
DoS-iFrameNet	N/A	CyberNotes-2003-04

Trojan	Version	CyberNotes Issue #
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	N/A	CyberNotes-2003-05
Downloader-BW.b	BW.b	CyberNotes-2003-06
Downloader-BW.c	BW.c	CyberNotes-2003-07
Exploit-IISInjector	N/A	CyberNotes-2003-03
Gpix	N/A	CyberNotes-2003-08
Hacktool.PWS.QQPass	N/A	CyberNotes-2003-06
ICQPager-J	N/A	CyberNotes-2003-05
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.ap	N/A	CyberNotes-2003-05
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC/Flood.br	br	CyberNotes-2003-06
IRC/Flood.bu	bu	CyberNotes-2003-08
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
IRC-Vup	**N/A**	**Current Issue**
JS.Fortnight.B	B	CyberNotes-2003-06
JS.Seeker.J	J	CyberNotes-2003-01
JS/Seeker-C	C	CyberNotes-2003-04
JS_WEBLOG.A	A	CyberNotes-2003-05
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Perfect.dr	**dr**	**Current Issue**
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
MultiDropper-FD	N/A	CyberNotes-2003-01
Pac	N/A	CyberNotes-2003-04
ProcKill-AE	N/A	CyberNotes-2003-05
ProcKill-AF	N/A	CyberNotes-2003-05
ProcKill-AH	AH	CyberNotes-2003-08
ProcKill-Z	N/A	CyberNotes-2003-03
Proxy-Guzu	N/A	CyberNotes-2003-08
PWS-Aileen	N/A	CyberNotes-2003-04
PWSteal.AlLight	N/A	CyberNotes-2003-01
PWSteal.Hukle	N/A	CyberNotes-2003-08
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWS-Tenbot	N/A	CyberNotes-2003-01
PWS-WMPatch	N/A	CyberNotes-2003-07
QDel359	359	CyberNotes-2003-01
QDel373	373	CyberNotes-2003-06
Qdel374	374	CyberNotes-2003-06
Qdel375	375	CyberNotes-2003-06
Qdel376	376	CyberNotes-2003-07
QDel378	378	CyberNotes-2003-08
QDel379	**369**	**Current Issue**

Trojan	Version	CyberNotes Issue #
Renamer.c	N/A	CyberNotes-2003-03
Reom.Trojan	N/A	CyberNotes-2003-08
StartPage-G	G	CyberNotes-2003-06
Stoplete	N/A	CyberNotes-2003-06
Swizzor	N/A	CyberNotes-2003-07
Tellafriend.Trojan	N/A	CyberNotes-2003-04
Tr/Decept.21	21	CyberNotes-2003-07
Tr/DelWinbootdir	N/A	CyberNotes-2003-07
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
Tr/SpBit.A	A	CyberNotes-2003-04
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Dloader-BO	N/A	CyberNotes-2003-02
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Slacker-A	A	CyberNotes-2003-05
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	A	CyberNotes-2003-04
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	A	CyberNotes-2003-05
Trojan.AprilFool	N/A	CyberNotes-2003-08
Trojan.Barjac	N/A	CyberNotes-2003-05
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Aphe	N/A	CyberNotes-2003-06
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Grepage	N/A	CyberNotes-2003-05
Trojan.Guapeton	N/A	CyberNotes-2003-08
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Uploader-D	D	CyberNotes-2003-06
Uploader-D.b	D.b	CyberNotes-2003-07
VBS.Kasnar	N/A	CyberNotes-2003-06
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02

Trojan	Version	CyberNotes Issue #
VBS.Trojan.Lovcx	N/A	CyberNotes-2003-05
VBS.Zizarn	**N/A**	**Current Issue**
VBS/Fourcourse	N/A	CyberNotes-2003-06
W32.Adclicker.C.Trojan	**C**	**Current Issue**
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CVIH.Trojan	N/A	CyberNotes-2003-06
W32.Noops.Trojan	**N/A**	**Current Issue**
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Systentry.Trojan	N/A	CyberNotes-2003-03
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32/Igloo-15	N/A	CyberNotes-2003-04
Xin	N/A	CyberNotes-2003-03

Backdoor.Assasin.F (Alias: Backdoor.Assasin.20): This is a variant of Backdoor.Assasin that gives a malicious user unauthorized access to a compromised computer. The existence of the file Ide.exe is an indication of a possible infection. This Trojan Horse is written in the Borland Delphi programming language and is compressed with UPX.

BackDoor-ATG: There are multiple variants of this Trojan, and the specific actions taken are decided by the malicious user who uses this Trojan, so this description is a general guide. As with most remote access Trojans, this threat appears to consists of multiple components: the configuration, client and server components. Once the server is running on the victim machine, the malicious user is able to connect (and administer that machine) using the client component. The configuration component would allow the malicious user to create slightly different versions of the Trojan. When run on the victim machine, the server component installs itself onto the system, typically copying itself to the Windows or System directory. For example, as C:\WINDOWS\SYSTEM\SHELL32EXEC.EXE. The server component can be used to offer many remote-administration functions to the malicious user. The server is added to an autostart registry key, though the values vary.

Backdoor.Bigfoot: This is a Backdoor Trojan that allows a malicious user to remotely control your computer. By default this Trojan opens port 2707 for listening. When Backdoor.Bigfoot is executed, it installs itself as the files:

- %System%\SystemTray.exe
- %System%\Sysstart.exe

and adds the value, “SystemTray"="%system%\SystemTray.exe,” to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

so that the Trojan runs each time you start Windows. It periodically searches for and terminates the processes with these filenames:

- Filemon.exe
- Regmon.exe

Backdoor.Kaitex.D: This is a Backdoor Trojan that uses a randomly changed TCP port to connect to the IRC servers of the malicious user choice. This Trojan allows the malicious user to remotely control the infected computer. When Backdoor.Kaitex.D runs, it adds the value, “Service"="<the Trojan file path and name>,” to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs each time you start Windows. The Trojan opens a randomly changed TCP port to connect to the IRC servers of the malicious user's choice and joins the #lerler IRC channel.

Backdoor.Kalasbot: This is a Backdoor Trojan Horse that allows a malicious user to control a compromised computer by using the Internet Relay Chat (IRC). When Backdoor.Kalasbot runs, adds a value, "Service"="<the Trojan file>," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you restart Windows. The Trojan registers itself as a service process under Windows 95/98/ME and opens randomly changed TCP/UDP ports to listen for commands from the malicious user. The commands allow the malicious user to perform various actions.

Backdoor.Litmus.203.c (Aliases: Backdoor.Litmus.203, BackDoor-JZ): This is a Backdoor Trojan that gives a malicious user access to your computer. The malicious user can control your computer using commands issued through IRC. When Backdoor.Litmus.203.c runs, it copies itself as %Windir%\Litmus\Mgodll.exe and creates the value, "LTM2"="%Windir%\Litmus\Mgodll.exe," in the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start Windows. Next it connects to an IRC server using port 6667, joins a specific channel, and notifies a malicious user by sending them a private message. Then, the Trojan waits for the commands that the malicious user transmits using IRC.

Backdoor.OptixPro.13 (Alias: Backdoor.Optix.Pro.13): This is a Trojan horse that gives a remote a malicious user full remote access to your computer. By default, the Trojan opens port 3410 for listening.

Backdoor.Pointex (Aliases: Backdoor.Pointex.c, Backdoor.Pointex.d): This is a Backdoor Trojan that gives a malicious user full access to your computer. The existence of the file Outlook32.exe is an indication of a possible infection. The Backdoor is written in Microsoft Visual Basic, version 6, and is packed with ASPack.

Backdoor.Pointex.B (Alias: Backdoor.Pointex.g): This is a variant of Backdoor.Pointex and gives a malicious user unauthorized access to your computer. It is written in Microsoft Visual Basic (VB) and compressed with ASPack. The VB run-time libraries are required for this Trojan Horse to be executed.

Backdoor.Ratega: This is a Trojan Horse that gives a malicious user complete access to your computer. By default, the Trojan listens on port 6969 and notifies the malicious user through e-mail. The Trojan notification message will contain the subject line "Omega Help." When Backdoor.Ratega is executed, it copies itself as %System%\WIN32.EXE and creates the files:

- %System%\Keylog.text
- %System%\Zlib.dll
- %WinDir%\Win32.dll

The Trojan adds the value, "WIN32"="%System%\WIN32.EXE," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that Backdoor.Ratega runs when you start Windows.

Backdoor.Recerv: This is a Trojan horse that gives a malicious user complete access to your computer. By default, the Trojan listens on port 9870 and notifies the malicious user through e-mail. The Trojan notification message will contain the subject line "R3C server - IP." When Backdoor.Recerv is executed, it copies itself as the following files:

- %WinDir%\Winsock.exe
- %System%\ipmon.exe

It adds the value, "ipmon.exe"="%System%\ipmon.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Backdoor.Recerv runs when you start Windows. This Trojan modifies the line in the [boot] section of the System.ini file to, "shell = Explorer.exe %windir%\winsock.exe," so that Backdoor.Recerv runs when you start Windows 95/98/ME.

Backdoor.Sdbot.H (Aliases: Backdoor.Sdbot.gen, IRC-Sdbot): This is a Backdoor Trojan that is a variant of Backdoor.Sdbot. It allows a malicious user to control a computer by using the Internet Relay

Chat (IRC). The existence of the file I3Explorer.exe is an indication of a possible infection. It can update itself by checking for newer versions over the Internet.

Backdoor.Simali: This is a Backdoor Trojan that gives a malicious user access to your computer. By default, the Trojan listens on port 22311 and on another configurable port. It attempts to notify the malicious user through e-mail or ICQ. Also, this threat is written in Delphi and is compressed with ASPack. When Backdoor.Simali is executed, it deletes the following files:

- %Windir%\Media\Start.wav
- %Windir%\Media\Windows XP Start.wav

Next is copies itself to the %System% folder as some of the following:

- Loader.exe
- Main.exe
- Lass.exe
- Msmsg.exe

and adds the value, "StubPath"="%system%\Loader.exe ok1," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Install Components\{6EF52A52-394A-11D3-B153-00707897TY}

so that the Trojan runs each time you start Windows. The Trojan also creates the following registry key and adds several values to it:

- HKEY_LOCAL_MACHINE\Software\XYKW42

The malicious user is notified through e-mail or ICQ.

BDS/Evilbot.A (Alias: Backdoor.Evilbot.a): Like other backdoors, BDS/Evilbot.A could potentially allow someone with malicious intent backdoor access to your computer. If executed, the Trojan adds the following file to the \windows\ directory, "msgrte.exe." So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "MSGRT"="C:\\WINDOWS\\MSGRTE.exe"

IRC-Vup: This detection is for an IRC Trojan that consists of multiple components, some of which are legitimate applications, that are dropped by a self-extracting executable dropper. The self-extracting dropper may vary in size and filename. When the dropper is run on the victim machine, numerous files are dropped (to the temporary directory in testing). Numerous files make up the package.

Keylog-Perfect.dr: This is a Trojanized deployment package for the Perfect Keylogger application. Such packages exist as self-extracting Rar archives. When run, a configurator-specified program is executed. Meanwhile, the Perfect Keylooger application is being installed in the background.

QDel379 (Aliases: Trj/W32.Boro, TROJ_PIKA.A): This Trojan written in Visual Basic delivers a file deletion payload when run on the victim machine. Upon execution, it attempts to delete various system files from the C:\WINDOWS directory (directory path is hardcoded in the Trojan). By deleting WIN.INI and SYSTEM.INI, the machine will fail to boot the next time. If any of the targeted files are not found, the program will stop executing and an error message will be displayed.

VBS.Zizarn: This is a Trojan Horse that tries to delete every file on every drive of your computer, including the floppy disks and network drives. This Trojan does not spread by itself. However, a malicious user or a program may send it as an e-mail attachment. When VBS.Zizarn is executed, it searches every available drive, including the local hard disks, floppy disks, and network drives, trying to delete every file that it finds. It starts with the current working folder, then recursively processes subfolders. If a file has the read only attribute, it will not be deleted. The Trojan may attempt to modify the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon

by adding the values:

- "LegalNoticeCaption" = "Legends of NR-Bio-Labs"
- "LegalNoticeText" = "Welcome to your Brand New Window :D"

W32.Adclicker.C.Trojan (Alias: AdClicker-C): This is a Trojan Horse that is designed to click on banner advertisements on certain Web pages. Most likely, these Web pages belong to the author of the Trojan. When W32.Adclicker.C.Trojan is executed, it attempts to generate clicks on banners at the following URLs:

- fastcounter.bcentral.com
- www.scorpionsearch.com
- hg1.hitbox.com

W32.Noops.Trojan: This is a Trojan Horse that deletes the system files and antivirus program files. It attempts to open the Web site, "www.porn.com." When W32.Noops.Trojan is executed, it attempts to delete the various files and sets the following values to "1:"

- "DisableTaskMgr"
- "DisableLockWorkstation"
- "DisableChangePassword"

under the registry key:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system

It also sets the following values to "1:"

- "NoLogoff"
- "NoClose"

under the registry key:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

and attempts to terminate the Norton AntiVirus AutoProtect service.